User Documentation – ME1310

Table of contents

Product description

Table of contents

ME1310 flexible edge server for rapid deployment of telecom and 5G services

The Kontron ME1310 high performance 1U edge server is a d istributed unit for wide temperature ranges . The ME1310 is used for RAN or multi-access edge computing (MEC). This platform has more cores, more memory and an increased density.

Main applications

- Solve restricted space and power challenges by enabling 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

- 3rd generation Intel® Xeon® D processor
- Two PCIe expansion slots for hardware acceleration
- On-board Ethernet network switch with PTP/SyncE and OCXO holdover
- Long product lifecycle
- Daisy chain configuration to connect multiple distributed units together
- Compliant with all major vRAN software
- DC or AC power
- Eight DDR4 DIMM sockets, 4 channels at up to 3200 MHz support up to 512GB
- Storage option:
  - Two M.2-2230 up to 512GB each and two M.2-2280 up to 2TB each (NVMe)
  - Four M.2-2230 up to 512GB each (NVMe)

Revision history

Revision	Brief description of changes	Date of issue
1.0	First client release	March 2023
1.1	• New portmaps in NOS release added to "Configuring the switch" • Corrected minimum fan speed in "Environmental considerations" • HCL: added M.2 2230 modules	

Warranty and support

Table of contents

Limited warranty

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

Disclaimer

Kontron would like to point out that the information contained in this manual may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the manual or any product characteristics set out in the manual. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this manual are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this manual only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

Customer support

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

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

For sales information, including current and future product options, please contact Kontron Sales Support in Canada through the following means:

- By phone: 1-800-387-4222
- By email: gss-com@kontron.com

Customer service

Kontron, a trusted technology innovator and global solutions provider, uses its embedded market strengths to deliver a service portfolio that helps companies break the barriers of traditional product lifecycles.

Through proven product expertise and collaborative, expert support, Kontron provides unparalleled peace of mind when it comes to building and maintaining successful products. To learn more about Kontron's service offering—including enhanced repair services, an extended warranty, and the Kontron training academy—visit www.kontron.com/support-and-services .

Safety and regulatory information

Table of contents

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

General safety warnings and cautions

⚠CAUTION	Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.
⚠WARNING	To prevent a fire or shock hazard, do not expose this product to rain or moisture. The chassis should not be exposed to dripping or splashing liquids and no objects filled with liquids should be placed on the chassis cover.
	ESD sensitive device! This equipment is sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.

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. 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.

WEEE directive logo

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.

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

Circuit overloading

Do not overload the circuits when connecting this product to the supply circuit as this can adversely affect overcurrent protection and supply wiring. Check the supply equipment nameplate ratings for correct use.

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.

⚠CAUTION	This equipment is designed for the earth grounded conductor (return) in the DC supply circuit to be connected to the earth grounding conductor on the equipment (ground lug).

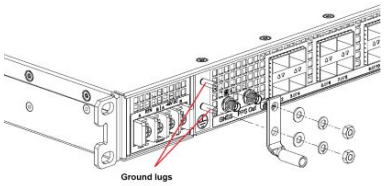
All of the following conditions must be met:

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.

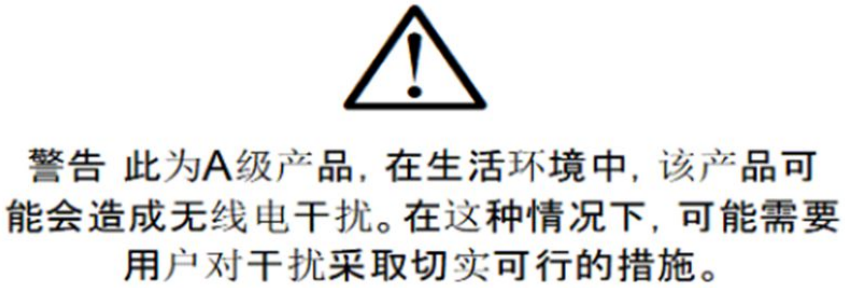
Reliable earth-grounding

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 ー A

Overview

Specifications

Table of contents

ME1310 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)

I/O	• 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:
	  ◦ Integrated 12-port Ethernet switch module (4x SFP28 , 8x SFP+)
	  ◦ Pass-through module with four 25 GbE SFP+ (This option is planned for development. Please contact Kontron sales .)

Timing	With Ethernet switch IO module option: • One SMA GNSS antenna input • One 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 4.0 (16GT/s) Refer to the Hardware compatibility list
CPU	Intel® Xeon® D-2700 family processors are supported, including the following processors: • Xeon® D-2796NT, 20 Cores @ 2.00GHz with QAT, 120 W • Xeon® D-2776NT, 16 Cores @ 2.10GHz with QAT, 117 W • Xeon® D-2776NT, 14 Cores @ 2.00GHz with QAT, 97 W
Storage	Two M.2 SSDs: • PCIe 3.0 x4 NVMe • Supported types: 2230 and 2280 Two M.2 SSDs: • PCIe 3.0 x2 NVMe • Supported types: 2230 Refer to the Hardware compatibility list
Memory	DDR4 DIMM with ECC • Bandwidth up to 3200 MT/s (minimum supported memory speed is 2400 MT/s) • Four memory channels • Two DIMM socket per channel Refer to the Hardware compatibility list
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 configuration • Automatic fan speed control
Rack mounting brackets	Front mount in a 19-in wide rack

ME1310 key software features

Feature	Description
Platform management	• BMC powered by OpenBMC • UEFI 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 enabled • Agent pre-provisioned
Operating system	Refer to the Validated operating systems
Thermal management	• Platform Environment Control Interface (PECI) for thermal management support • Memory and CPU thermal management

ME1310 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]	

ME1310 packaging physical dimensions

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

ME1310 shipping weights

Component	Weight (kg [lb])
AC PSU system weight – with four DIMMs and one M.2-2280 SSD	6.93 [15.3]
DC PSU system weight – with four DIMMs and one M.2-2280 SSD	6.79 [15.0]
Packaging (box + foam + bag)	1.59 [3.5]

ME1310 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 g^2/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 g^2/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.

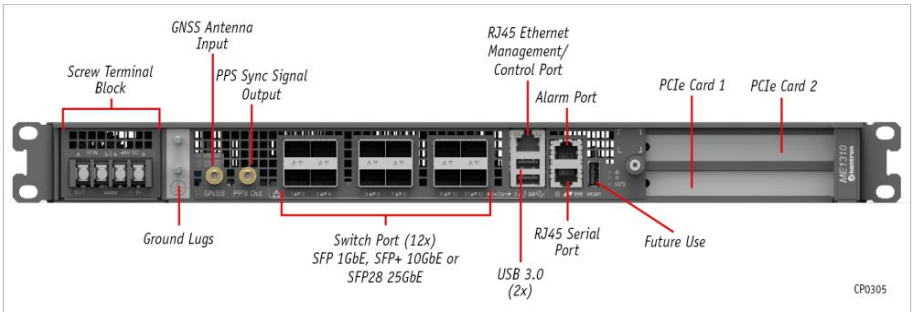
Platform components

Table of contents

Platform front panel

The ME1310 platform is 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 Connector pinouts and electrical characteristics .
For information on cabling, refer to Cabling .

Ethernet switch IO module option

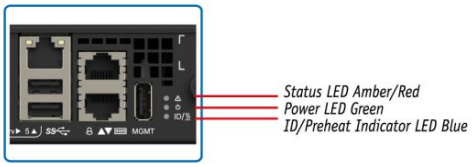


Pass-through IO module option

This option is planned for development. Please contact Kontron sales .

Platform LEDs

General platform LEDs



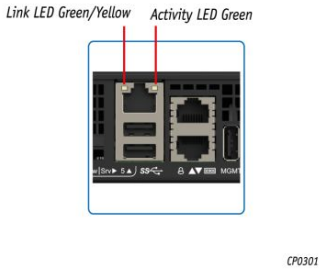
Status (amber/red)	State
Off	No active error notification (normal operation)
Amber On	Major alarm active
Red On	Critical alarm active (service/maintenance is required)

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 blink	Server processor activation complete and executing – ACPI Working state (S0)
Off	Normal blink	UEFI/BIOS started POST
Off	Normal blink or On [1]	UEFI/BIOS hand over to OS boot loader
Off	On [1]	Application started/running OK

[1] By default, the Power LED will be set by the UEFI/BIOS to "On" when the integrated server OS boot loader is launched. Via a UEFI/BIOS setting, the Power LED can remain in "Normal blink" until customer application confirms it is running by setting an I/O register bit. Refer to Configuring option Application Ready LED in section Configuring UEFI/BIOS options and to Platform resources for customer application to view a code example 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

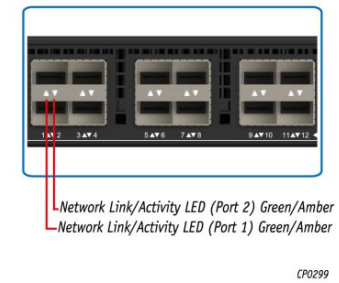
Network port Srv 5 LEDs



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

Ethernet switch module



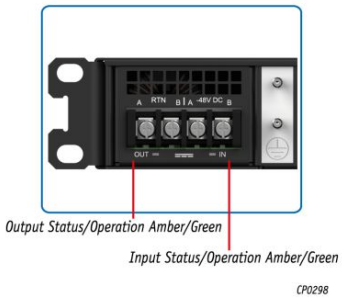
Network link/activity (green/amber)	State
Green On	Link established at maximum port speed (10 or 25Gbps), no activity
Amber On	Link established at below maximum port speed (e.g. link is at 1Gbps on a 10Gpbs port) , no activity
Blinking (green or amber based on port speed)	Activity
Off	No link

Pass-through module

This option is planned for development. Please contact Kontron sales .

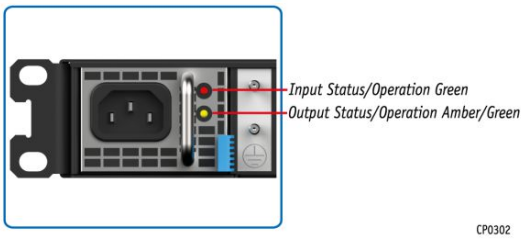
Power supply LEDs

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 Components installation and assembly 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

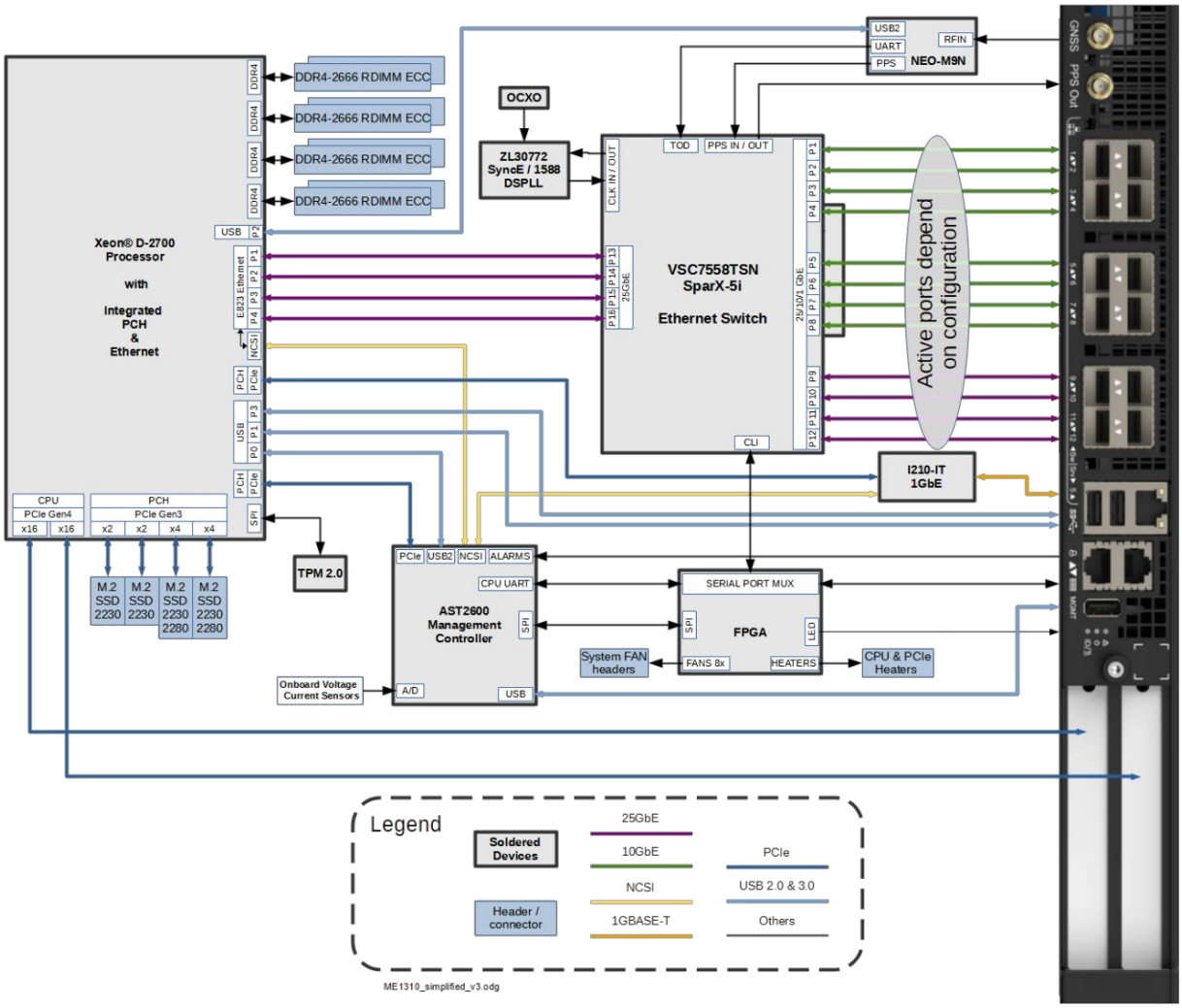
Relevant section:
MAC addresses (for QR code results, which include the serial number)

Product architecture

Table of contents

Block diagram

Block diagram with the Ethernet switch IO module option



Block diagram with the p ass-through IO module option

This option is planned for development. Please contact Kontron sales .

Network planes

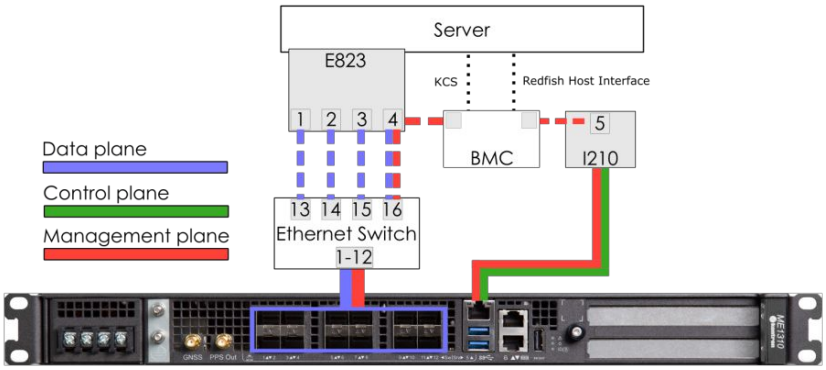
The ME1310 platform provides:

- **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 w ith the Ethernet switch IO module option



Internal connections with the p ass-through IO module option

This option is planned for development. Please contact Kontron sales .

Description of system access methods

Table of contents

To configure, monitor and troubleshoot the ME1310 platform and its components, several interfaces can be used:

- **Management interface (BMC)** – through the management plane and the data plane of the platform
- **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
- **Switch network operating system (NOS)** (on platforms equipped with the Ethernet switch IO module) – 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 (BMC)	
Path description	**Main reasons for use**
BMC Web UI *This is the recommended path for first time out-of-the-box system configuration.* *Accessible from the BMC management plane.*	• Remote server control and monitoring • OS video access • Firmware upgrades
Redfish *This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.* *Accessible from the BMC management plane, and locally from the server operating system via the Redfish host interface.*	• Remote server monitoring • Remote server control • Firmware upgrades
IPMI over LAN (IOL) *This is a good path for automated monitoring/control script once the platform has been configured for the first time.* *Accessible from the BMC management plane .*	• 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 Accessing the operating system of a server .

Paths to the operating system	
Path description	**Main reasons for use**
KVM *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 BMC management plane.*	• 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 BMC 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 BMC 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 BMC management plane.*	• OS network interface configuration • Unable to establish a network session to the OS • OS serial console access
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

*Note that communication with the BMC management plane via the integrated switch can be lost because of configurations applied in the NOS.

Note that communication with the BMC management plane via the integrated switch can be lost because of configurations applied in the NOS.

Paths to the UEFI/BIOS options

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

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 BMC 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 BMC management plane.*	• Initial UEFI/BIOS configuration • UEFI/BIOS video access
Serial over LAN using SSH from a remote computer *Accessible from the BMC 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 BMC 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 BMC 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

*Note that communication with the BMC management plane via the integrated switch can be lost because of configurations applied in the NOS.

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 NOS 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 monitoring • Firmware upgrades
Serial over LAN using the BMC Web UI *Accessible from the BMC management plane.*	• NOS network interface configuration • Initial switch NOS configuration
Serial over LAN using SSH from a remote computer *Accessible from the BMC management plane.*	• NOS network interface configuration • Initial switch NOS configuration
SSH from a remote computer *This is a good path for automated monitoring/control script once the platform has been configured for the first time.* *Accessible from the data plane.*	• Switch NOS control and monitoring • Firmware upgrades
SSH from the integrated server *Accessible locally from the server operating system.*	• Local access to the s witch NOS for control and 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

The ME1310 platform has been designed to work over the extended temperature range of -40ºC to +65ºC (-40ºF to +149ºF) when using a DC power supply or -5ºC to +50ºC (23ºF to +122ºF) 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, an appropriate housing must be used.

If components that do not support the ME1310 temperature range are installed, the customer is responsible to configure sensor thresholds and thermal management accordingly. Refer to Configuring sensors and thermal parameters and Platform cooling and thermal management .

When powering up the ME1310 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. Please refer to Platform cooling and thermal management for more information.

Special considerations must be taken if you are exposing the ME1310 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 ME1310 in a hot environment, it is recommended to take additional measures to maximize the cooling and air circulation as a constant exposure to high temperatures reduces the life expectancy of electronic equipment.

The ME1310 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

DC power supply input voltage and current requirements

Relevant section:
Cabling

Mating connector: Refer to the Cabling section 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 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 ME1310 configuration was used to obtain the typical power consumption values shown in the table below:

- Xeon® D-2796NT processor
- Ethernet switch IO module with standard OCXO
- Eight 64 GB LRDIMM
- One 128 GB M.2 NVMe 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	78	Idle power consumption was measured in CentOS 7 once it had finished booting
Maximum application	342	Maximum power was measured in CentOS 7 running "mprime -t" as a stress application
Maximum application and fan	500	Maximum power was measured in CentOS 7 running "mprime -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-2796NT	120	TDP
Intel ® Xeon ® D-2776NT	117	TDP
Intel ® Xeon ® D-2766NT	97	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
NVMe 128GB, 512GB, 1TB or 2TB M.2 SSD	7	Under active use. Idle power is 1 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 co uld exceed its maximum power consumption.

MAC addresses

Table of contents

Relevant section:
Product architecture

MAC addresses

Ethernet switch IO module option

MAC address	Interface description	Device	Note
MAC_BASE	Front panel Srv 5	BMC	Shared connector with server.
MAC_BASE + 1	Server internal port 4	BMC	Internal to switch interface 1/16 . Shared connection with server.
MAC_BASE + 2	Server Redfish host interface	Server	Internal to BMC via integrated USB-LAN .
MAC_BASE + 3	Server internal port 1	Server	Internal to switch interface 1/13.
MAC_BASE + 4	Server internal port 2	Server	Internal to switch interface 1/14.
MAC_BASE + 5	Server internal port 3	Server	Internal to switch interface 1/15.
MAC_BASE + 6	Server internal port 4	Server	Internal to switch interface 1/1 6 . Shared connection with BMC .
MAC_BASE + 7	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 + 1 to SW_MAC_BASE + 17	Reserved	Switch NOS	Reserved MAC for switch network operating system.

Pass-through IO module option

This option is planned for development. Please contact Kontron sales .

Discovering the platform MAC addresses

The platform MAC addresses can be discovered:

- Using the QR code
- Using the UEFI/BIOS

Discovering a MAC address using the QR code

Step_1	Using a QR code application, scan the QR code of the platform. Record the information obtained in your device (e.g. by taking a screen shot).
	
	S/N:9017020001 = Platform serial number
	P/N:1065-2823 = Platform part number
	BATCH:0A00000001 = Platform production lot number
	MAC:
	00A0A5D6402A = First MAC address attributed to the BMC/server. Value to be used to replace MAC_BASE.
	00A0A5E1B934 = First MAC address attributed to the integrated Ethernet switch. Value to be used to replace SW_MAC_BASE. This is only present for a platform configured with the IO Ethernet switch module.
		`S/N:9017020001`
		`P/N:1065-2823`
		`BATCH:0A00000001`
		`MAC:`
		`00A0A5D6402A`
		`00A0A5E1B934`

Discovering a MAC address using the UEFI/BIOS

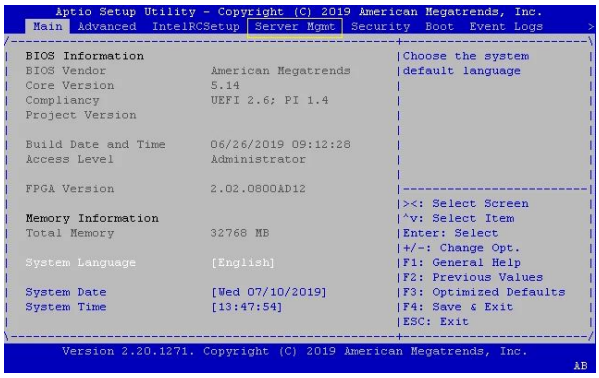
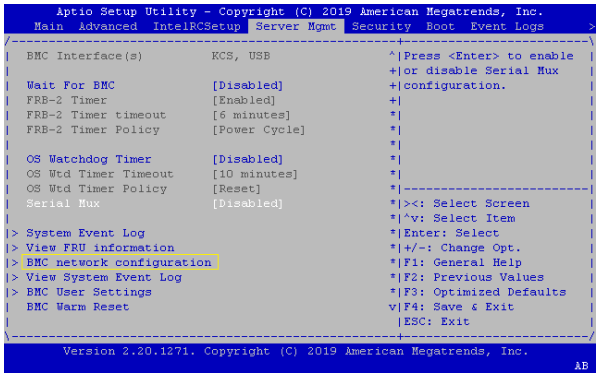
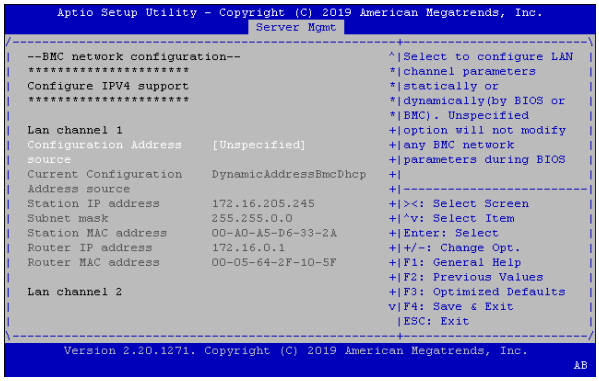
Prerequisites

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 Accessing the UEFI/BIOS for access instructions.

Step_1	From the UEFI/BIOS menu, navigate to tab **Server Mgmt** .	
Step_2	Select **BMC network configuration** .	
Step_3	The **BMC network configuration** menu is displayed. **NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS .	

PCI mapping

Table of contents

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

Platform PCI mapping

Bus: Device. Function	Vendor ID	Device ID	Component	Description
00:00.0	8086	09a2	System peripheral	Intel Corporation Device
00:00.1	8086	09a4	System peripheral	Intel Corporation Device
00:00.2	8086	09a3	System peripheral	Intel Corporation Device
00:00.3	8086	09a5	System peripheral	Intel Corporation Device
00:00.4	8086	0998	Host bridge	Intel Corporation Device
00:01.0	8086	0b00	System peripheral	Intel Corporation Device
00:01.1	8086	0b00	System peripheral	Intel Corporation Device
00:01.2	8086	0b00	System peripheral	Intel Corporation Device
00:01.3	8086	0b00	System peripheral	Intel Corporation Device
00:01.4	8086	0b00	System peripheral	Intel Corporation Device
00:01.5	8086	0b00	System peripheral	Intel Corporation Device
00:01.6	8086	0b00	System peripheral	Intel Corporation Device
00:01.7	8086	0b00	System peripheral	Intel Corporation Device
00:02.0	8086	09a6	System peripheral	Intel Corporation Device
00:02.1	8086	09a7	System peripheral	Intel Corporation Device
00:02.4	8086	3456	Non-Essential Instrumentation	Intel Corporation Device
00:09.0	8086	18a4	PCI bridge	Intel Corporation Device
00:0b.0	8086	18a6	PCI bridge	Intel Corporation Device
00:0f.0	8086	18ac	System peripheral	Intel Corporation Device
00:16.0	8086	18af	PCI bridge	Intel Corporation Device
00:17.0	8086	18a2	PCI bridge	Intel Corporation Device
00:18.0	8086	18d3	Communication controller	Intel Corporation Device
00:18.1	8086	18d4	Communication controller	Intel Corporation Device
00:18.4	8086	18d6	Communication controller	Intel Corporation Device
00:1a.0	8086	18d8	Serial controller	Intel Corporation Device
00:1a.1	8086	18d8	Serial controller	Intel Corporation Device
00:1a.2	8086	18d8	Serial controller	Intel Corporation Device
00:1a.3	8086	18d9	Unassigned class	Intel Corporation Device
00:1d.0	8086	0998	Host bridge	Intel Corporation Device
00:1e.0	8086	18d0	USB controller	Intel Corporation Device
00:1f.0	8086	18dc	ISA bridge	Intel Corporation Device
00:1f.4	8086	18df	SMBus	Intel Corporation Device
00:1f.5	8086	18e0	Serial bus controller	Intel Corporation Device
00:1f.7	8086	18e1	Non-Essential Instrumentation	Intel Corporation Device
01:00.0	1d79	2263	Non-Volatile memory controller	Transcend Information, Inc. Device

02:00.0	1a03	1150	PCI bridge	ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge
03:00.0	1344	6001	Non-Volatile memory controller	Micron Technology Inc Device
04:00.0	8086	1533	Ethernet controller	Intel Corporation I210 Gigabit Network Connection
05:00.0	1a03	2000	VGA compatible controller	ASPEED Technology, Inc. ASPEED Graphics Family
15:00.0	8086	09a2	System peripheral	Intel Corporation Device
15:00.1	8086	09a4	System peripheral	Intel Corporation Device
15:00.2	8086	09a3	System peripheral	Intel Corporation Device
15:00.3	8086	09a5	System peripheral	Intel Corporation Device
15:00.4	8086	0998	Host bridge	Intel Corporation Device
15:02.0	8086	347a	PCI bridge	Intel Corporation Device
16:00.0	8086	0d5c	Processing accelerators	Intel Corporation Device
80:00.0	8086	09a2	System peripheral	Intel Corporation Device
80:00.1	8086	09a4	System peripheral	Intel Corporation Device
80:00.2	8086	09a3	System peripheral	Intel Corporation Device
80:00.3	8086	09a5	System peripheral	Intel Corporation Device
80:00.4	8086	0998	Host bridge	Intel Corporation Device
80:05.0	8086	18da	PCI bridge	Intel Corporation Device
81:00.0	8086	18a0	Co-processor	Intel Corporation C4xxx Series QAT
88:00.0	8086	09a2	System peripheral	Intel Corporation Device
88:00.1	8086	09a4	System peripheral	Intel Corporation Device
88:00.2	8086	09a3	System peripheral	Intel Corporation Device
88:00.3	8086	09a5	System peripheral	Intel Corporation Device
88:00.4	8086	0998	Host bridge	Intel Corporation Device
88:04.0	8086	18d1	PCI bridge	Intel Corporation Device
89:00.0	8086	188a	Ethernet controller	Intel Corporation Ethernet Connection E823-C for backplane
89:00.1	8086	188a	Ethernet controller	Intel Corporation Ethernet Connection E823-C for backplane
89:00.2	8086	188a	Ethernet controller	Intel Corporation Ethernet Connection E823-C for backplane
89:00.3	8086	188a	Ethernet controller	Intel Corporation Ethernet Connection E823-C for backplane
90:00.0	8086	09a2	System peripheral	Intel Corporation Device
90:00.1	8086	09a4	System peripheral	Intel Corporation Device
90:00.2	8086	09a3	System peripheral	Intel Corporation Device
90:00.3	8086	09a5	System peripheral	Intel Corporation Device
90:00.4	8086	0998	Host bridge	Intel Corporation Device
90:02.0	8086	347a	PCI bridge	Intel Corporation Device
fe:00.0	8086	3450	System peripheral	Intel Corporation Device
fe:00.1	8086	3451	System peripheral	Intel Corporation Device
fe:00.2	8086	3452	System peripheral	Intel Corporation Device
fe:00.3	8086	0998	Host bridge	Intel Corporation Device
fe:00.5	8086	3455	System peripheral	Intel Corporation Device
fe:0b.0	8086	3448	System peripheral	Intel Corporation Device
fe:0b.1	8086	3448	System peripheral	Intel Corporation Device
fe:0b.2	8086	344b	System peripheral	Intel Corporation Device
fe:0c.0	8086	344a	Performance counters	Intel Corporation Device
fe:0d.0	8086	344a	Performance counters	Intel Corporation Device
fe:1a.0	8086	2880	Performance counters	Intel Corporation Device

fe:1b.0	8086	2880	Performance counters	Intel Corporation Device
ff:00.0	8086	344c	System peripheral	Intel Corporation Device
ff:00.1	8086	344c	System peripheral	Intel Corporation Device
ff:00.2	8086	344c	System peripheral	Intel Corporation Device
ff:00.3	8086	344c	System peripheral	Intel Corporation Device
ff:00.4	8086	344c	System peripheral	Intel Corporation Device
ff:00.5	8086	344c	System peripheral	Intel Corporation Device
ff:00.6	8086	344c	System peripheral	Intel Corporation Device
ff:00.7	8086	344c	System peripheral	Intel Corporation Device
ff:01.0	8086	344c	System peripheral	Intel Corporation Device
ff:01.1	8086	344c	System peripheral	Intel Corporation Device
ff:01.2	8086	344c	System peripheral	Intel Corporation Device
ff:01.3	8086	344c	System peripheral	Intel Corporation Device
ff:0a.0	8086	344d	System peripheral	Intel Corporation Device
ff:0a.1	8086	344d	System peripheral	Intel Corporation Device
ff:0a.2	8086	344d	System peripheral	Intel Corporation Device
ff:0a.3	8086	344d	System peripheral	Intel Corporation Device
ff:0a.4	8086	344d	System peripheral	Intel Corporation Device
ff:0a.5	8086	344d	System peripheral	Intel Corporation Device
ff:0a.6	8086	344d	System peripheral	Intel Corporation Device
ff:0a.7	8086	344d	System peripheral	Intel Corporation Device
ff:0b.0	8086	344d	System peripheral	Intel Corporation Device
ff:0b.1	8086	344d	System peripheral	Intel Corporation Device
ff:0b.2	8086	344d	System peripheral	Intel Corporation Device
ff:0b.3	8086	344d	System peripheral	Intel Corporation Device
ff:1d.0	8086	344f	System peripheral	Intel Corporation Device
ff:1d.1	8086	3457	System peripheral	Intel Corporation Device
ff:1e.0	8086	3458	System peripheral	Intel Corporation Device
ff:1e.1	8086	3459	System peripheral	Intel Corporation Device
ff:1e.2	8086	345a	System peripheral	Intel Corporation Device
ff:1e.3	8086	345b	System peripheral	Intel Corporation Device
ff:1e.4	8086	345c	System peripheral	Intel Corporation Device
ff:1e.5	8086	345d	System peripheral	Intel Corporation Device
ff:1e.6	8086	345e	System peripheral	Intel Corporation Device
ff:1e.7	8086	345f	System peripheral	Intel Corporation Device

Connector pinouts and electrical characteristics

Table of contents

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

Relevant sections:

Platform components

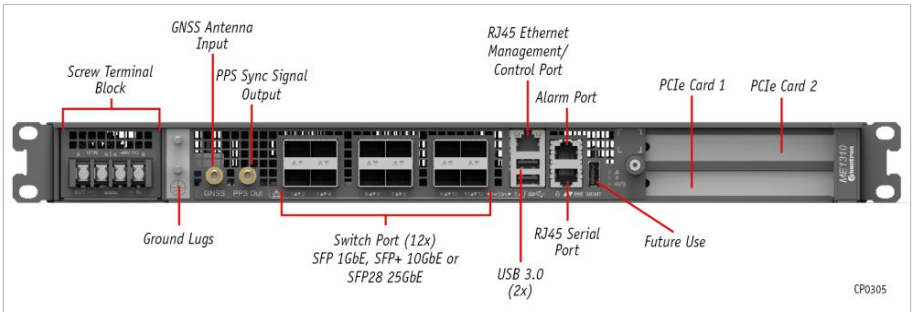
Cabling

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

NOTICE	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

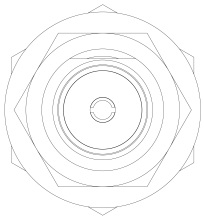
This option is planned for development. Please contact Kontron sales .

Description, pinout and electrical characteristics of external connectors

This section describes the following connectors and lists their pinouts and electrical characteristics:

- 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
- Alarm connector
- 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



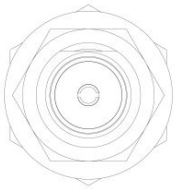
Mating connector: SMA Male

Description:

- Integrated NEO-M9N GNSS receiver antenna input
- 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
  - 5 V ± 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:
Cabling

SMA PPS output



Mating connector: SMA Male

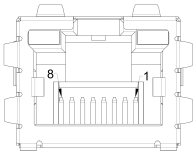
Description:

- 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:
  - $V_{OH} > 2.6$ V at $I_{OH} = -12$ mA
  - $V_{OL} < 0.7$ 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

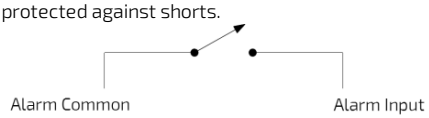
Alarm connector

If the alarm connector is not used, TelcoAlarm sensors should be disabled, so no open loop event is generated in the BMC system event log upon BMC reboot.
Another solution would be to install a loop back connector assembly into the alarm connector.

Relevant sections:
Configuring sensors and thermal parameters (to enable or disable TelcoAlarm sensors)
Monitoring sensors (to view TelcoAlarm sensor statuses)



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



Open circuit voltage:

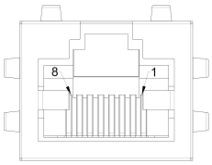
- ALARM_CM: 5 V to 7 V, current limited to < 60 mA
- ALARM_IN[7:1]: -7 V to -5 V, 10 kiloohms impedance

External connector pinout

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

Relevant sections:
Discrete sensor monitoring procedure
Interpreting sensor data

RJ45 serial port



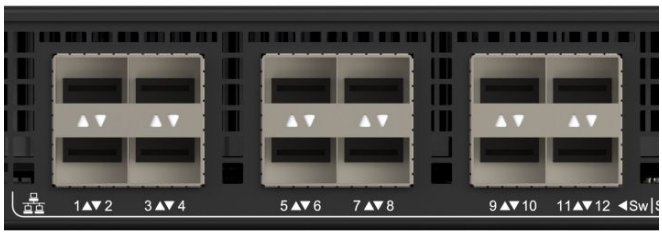
Description:
The serial port is electrically compatible to standard RS-232.

External connector pinout:

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 Configuring the switch for information on how to configure the port map.
Mating connector: SFP+ or SFP28 modules

Pass-through IO module option

This option is planned for development. Please contact Kontron sales .

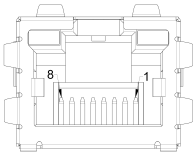
Description:
The SFP+ and SFP28 interfaces are standardized and are compliant to the following (non exhaustive):

- SFF-8431, SFF-8432 (SFP+)
- SFF-8402 (SFP28)
- 1000BASE-LX/SX, SFP-MSA, SFF INF-8074i (all IO module options)
- 10GBASE-CR/LR/SR, IEEE802.3 clause 52 (all IO module options)
- 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

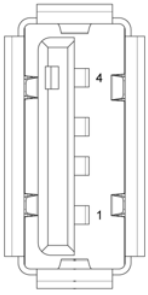


Description:
This interface is a standard 10/100/1000 Base-T port and is compliant to the following (non exhaustive):

- IEEE 802.3 clause 40

NOTICE	A cable length up to 100 meters is acceptable for intra-building connections if the installation conforms to Telcordia GR-1089 issue 6 for type 2 port with longitudinal lightning surge test exemption (section 4.5.3.1).

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 USB Implementers Forum .

DC power supply input connector

Mating connector: Refer to the Cabling section to build appropriate cables.

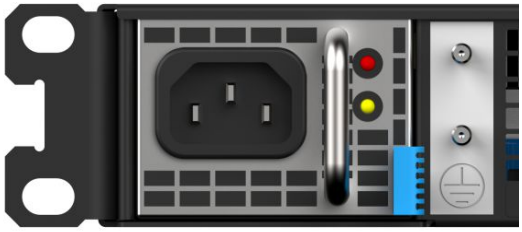
Description:
The DC power input is designed in accordance with Telcordia GR-1089 and ATIS-0600315 and has the following characteristics:

- 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)

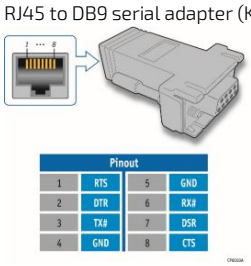
Material, information and software required

Table of contents

Material and information required

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

Optional adapter

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

Component installation and assembly

PCIe 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.

Item_1	One T10 Torx screwdriver
Item_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

For a DC PSU

Item_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)
Item_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
Item_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
Item_6	One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)
Item_7	One hand crimp tool, Panduit CT-1700
Item_8	7 mm wrench or equivalent tool

For an AC PSU

Item_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

Item_1	Racking fasteners (rack specific)

Network cables and modules

Ethernet switch IO module option

Item_1	One SFP optical module (SX, LX, SR, LR) with compatible optical cable
Item_2	One RJ45 Ethernet management/control plane cable
Item_3	One RJ45 serial connection cable

Pass-through IO module option

This option is planned for development. Please contact Kontron sales .

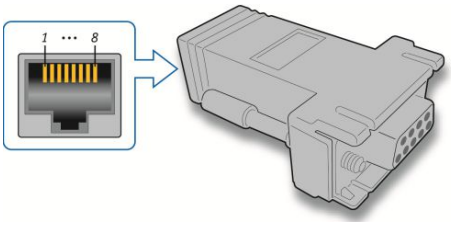
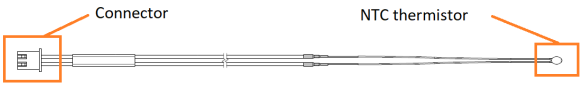
Software required

Item_1	An HTTP client such as **cURL** or **Postman** is recommended for using the platform Redfish interface. Throughout the documentation, **cURL** will be used.
Item_2	A terminal emulator such as **PuTTY** is installed on a remote computer.
Item_3	A hardware detection tool such as **pciutils** is installed on the local server to view information about devices connected to the server PCI buses .
Item_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

Relevant section:
Components installation and assembly

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

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

Hardware compatibility list

Table of contents

M.2 industrial SSDs (-40°C to 85°C)

Type	Size	Dimension	Vendor	Vendor P/N	Status	Kontron P/N
NVMe	128GB	2280	Transcend	TS128GMTE652TI	Active	1068-6586
NVMe	256GB	2230	Kioxia	KAG12ZNS256G	Active	1069-6771
NVMe	512GB	2230	Kioxia	KAG12ZNS512G	Active	1069-6775
NVMe	512GB	2280	Transcend	TS512GMTE652TI-KCI	Active	1068-1170
			Western Digital	SDBPNPZ-512G-XI	Active	
NVMe	1TB	2280	Transcend	TS1TMTE662TI-KCI	Active	1068-1161
			Western Digital	SDBPNPZ-1T00-XI	Active	
NVMe	2TB	2280	Transcend	TS2TMTE662TI-KCI	Active	1068-1158
			Western Digital	SDBPNPZ-2T00-XI	Active	

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

Size	Type	Vendor	Vendor P/N	Status	Kontron P/N
16GB	DDR4-3200*	Micron Technology	MTA18ASF2G72PDBZ-3G2E1	Active	1067-0181
32GB	DDR4-3200*	Micron Technology	MTA36ASF4G72PBZ-3G2E1	Active	1068-6284
64GB	DDR4-3200*	Smart Modular Technology	STI8197RD440425-SA	Active	1068-6291

*ME1310 platforms support DDR4 speeds of up to 2933

SFP, SFP+ and SFP28 industrial modules (-40°C to 85°C)

Modules shall be tested:

- With the Ethernet switch IO module in ports configured to support the module speed grade

Type	Vendor	Vendor P/N	Description	Status	Kontron P/N
1000BASE-SX	II-VI (Finisar)	FTLF8519P3BTL	500m, 850nm, -40°C to 85°C, SFP optical transceiver	Active	1064-5770
10GBASE-SR	II-VI (Finisar)	FTLX8573D3BTL	400m, 850nm, -40°C to 85°C, SFP+ optical transceiver	EOL	1064-5765
	II-VI (Finisar)	FTLX8574D3BTL	400m, 850nm, -40°C to 85°C, SFP+ optical transceiver	Active	
	FormericaOE	TAS-A2NH1-P11	300m, 850nm, -40°C to 85°C, SFP+ optical transceiver	Active	
25GBASE-SR	FS	SFP28-25GSR-85-I	100m, 850nm, -40°C to 85°C, SFP28 optical transceiver	Active	1068-5031
	II-VI (Finisar)	FTLF8536W4BTV	100m, 850nm, -40°C to 85°C, SFP28 optical transceiver	Active	
1000BASE-LX	FormericaOE	TSD-S2CA1-F11	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	1065-3758
	II-VI (Finisar)	FTLF1318P3BTL	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	
	Avago	AFCT-5715ALZ	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	
10GBASE-LR	FS	SFP-10GLR-31-I	10Km, 1310nm, -40°C to 85°C, SFP+ optical transceiver	Active	1065-6804
	II-VI (Finisar)	FTLX1475D3BTL	10Km, 1310nm, -40°C to 85°C, SFP+ optical transceiver	Active	
25GBASE-LR	FS	SFP28-25GLR-31-I	10Km, 1310nm, -40°C to 85°C, SFP28 optical transceiver	Active	1068-5037

Validated operating systems

Table of contents

Status description

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

OS certification status

NOTE: Contact Customer support for additional operating system certification or validation.

Operating system	Status
CentOS 7.8	PLANNED
RHEL 7.8	PLANNED
RHEL 8.2	PLANNED
SUSE EL 15 SP2	PLANNED
Ubuntu 18.04	PLANNED
Ubuntu 20.04	PLANNED
VMWare ESXi 6.7	PLANNED

Security

- Establish a plan to change default user names and password. Refer to Configuring and managing users .
- Determine the access paths that are to be closed or open. Refer to the children sections of Configuring networking .
- The BMC SNMP service is enabled by default. Minimally set the community string to a unique value or disable the service. Refer to Configuring BMC SNMP .
- The platform supports Secure Boot. Refer to Configuring UEFI/BIOS options .
- 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 Configuring UEFI/BIOS options .

For more information on security features, contact Kontron.

Getting started - Application installation and performance benchmarking

Table of contents

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

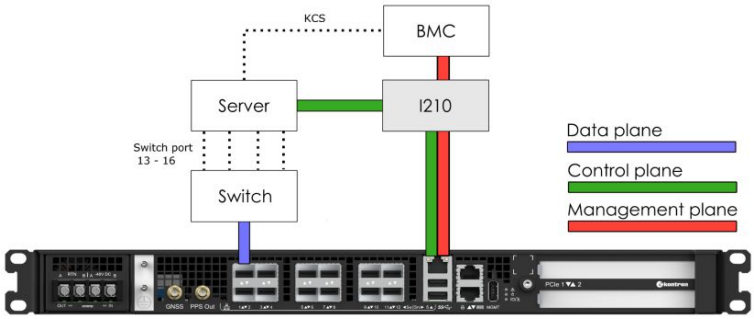
This getting started section describes the network integration, platform access and operating system installation steps required to start operating an ME1310 platf orm equipped with one or two PCIe add-in cards provided b y the customer and o ne 128GB M.2 SATA drive, and used to leverage two segregated 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:
  - 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 switch port 1 (**Sw 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 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

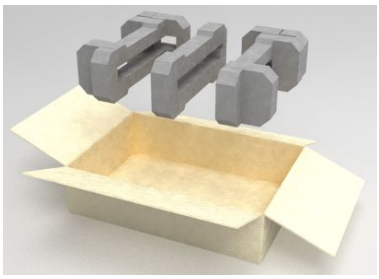
Network integration summary



Unboxing the platform

What's in the box

The box includes **one ME1310 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 Material and information required for more information).

Planning

Material and information required

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

PCIe add-in card

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

Item_1	One T10 Torx screwdriver
Item_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

Item_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)
Item_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
Item_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
Item_6	One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)
Item_7	One hand crimp tool, Panduit CT-1700
Item_8	7 mm wrench or equivalent tool

Rack installation material

Item_1	Racking fasteners (rack specific)

Network cables and modules

Item_1	One SFP optical module (SX, LX, SR, LR) with compatible optical cable
Item_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

Software required

Relevant section:
Common software installation

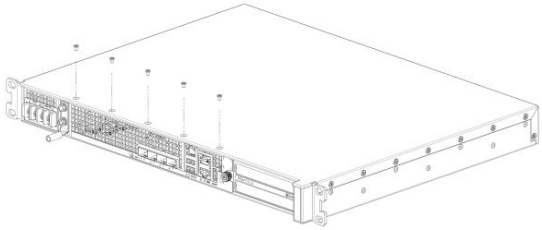
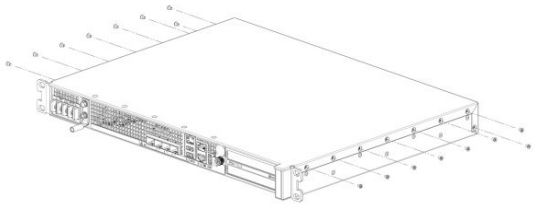
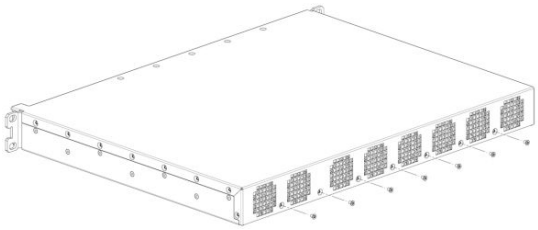
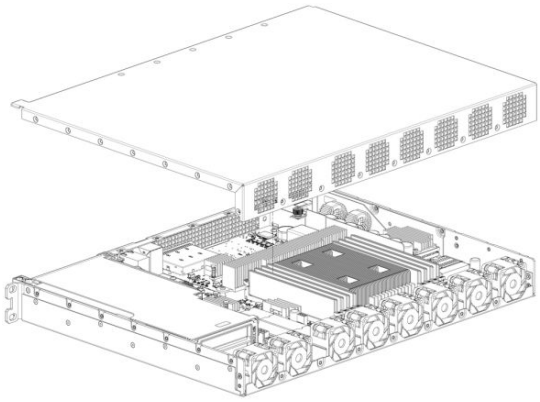
Item_1	An HTTP client such as **cURL** or **Postman** is recommended for using the platform Redfish interface. Throughout the documentation, **cURL** will be used.
Item_2	A terminal emulator such as **PuTTY** is installed on a remote computer.
Item_3	A hardware detection tool such as **pciutils** is installed on the local server to view information about devices connected to the server PCI buses .
Item_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 ME1310

	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

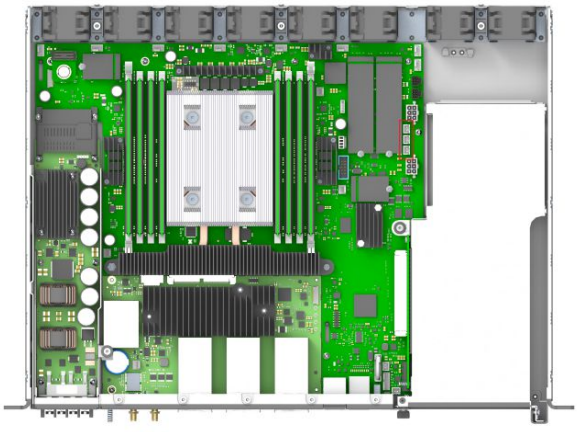
Step_1	Remove the 5 screws from the top using a T10 Torx screwdriver.	
Step_2	Remove the 16 screws from the sides (8 per side) using a T10 Torx screwdriver.	
Step_3	Remove the 7 screws from the back using a T10 Torx screwdriver .	
Step_4	Lift the cover up to remove it.	

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 ME1310.

Location	Reference designator	Connector
Back	J20	PCIe slot 1
Middle	J21	PCIe slot 2
Front	J23	Chassis



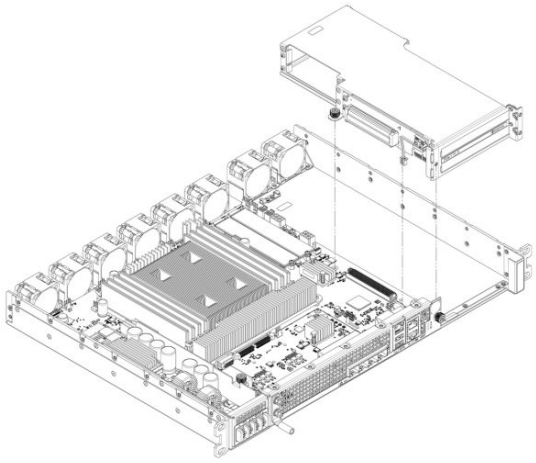
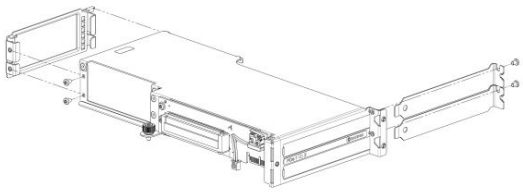
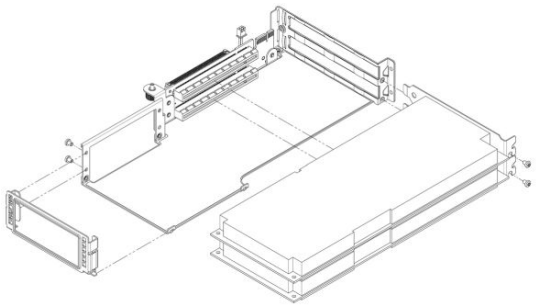
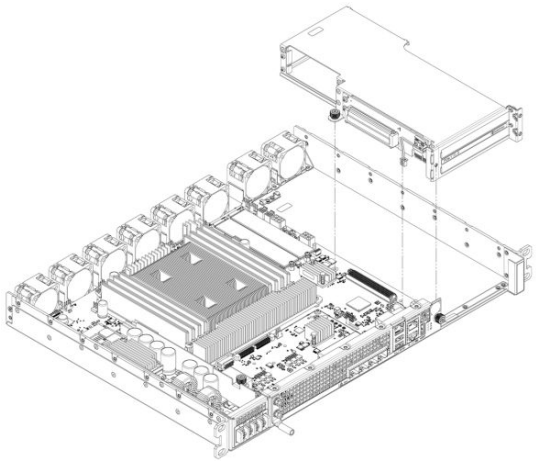
Installing the thermal probes

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.

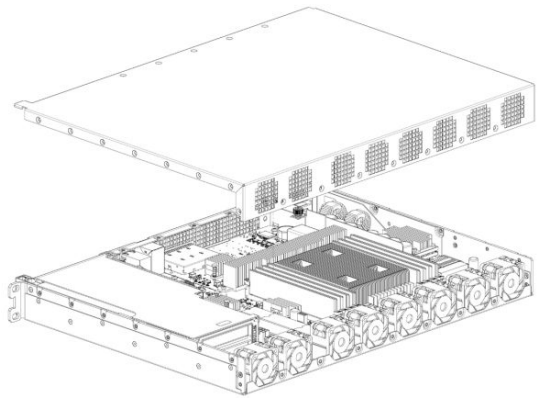
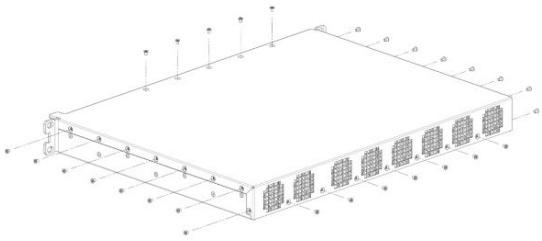
Refer to Configuring sensors and thermal parameters to configure thermal parameters.

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).

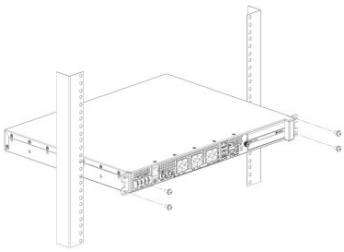
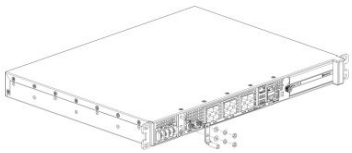
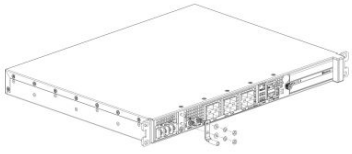
Step_1	Using a T10 Torx screwdriver, unfasten the two thumbscrews located in the front of the chassis a nd on the main board . Disconnect the intrusion detection switch wire near the front of the chassis. Lift the PCIe assembly out of the chassis.	
Step_2	Using a T10 Torx screwdriver, remove one PCIe 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 lbs-in torque) . Mount the PCIe rear holder onto the assembly and tighten the M3 screws with a T10 Torx screwdriver (6 lbs-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 lbs-in torque). Connect the intrusion detection switch wire near the front of the chassis.	

Closing the chassis

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).	

Racking the platform

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

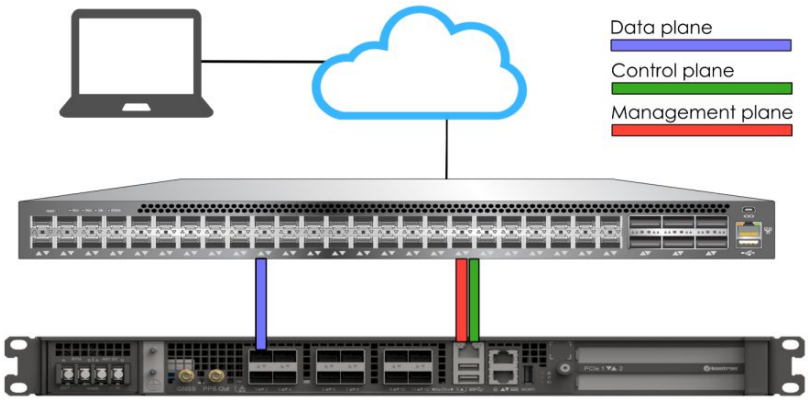
Step_1	Choose a location for the platform in the rack.	
Step_2	Insert the platform in the rack.	
Step_3	Fasten the platform to the rack using the appropriate fasteners.	
Step_4	If a ground lug is installed, remove the 2 nuts and washers from the ground lug studs. Take out the ground lug.	
Step_5	Strip 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).	
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

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 (**Srv 5**).
Step_2	Connect one SFP or SFP+ cable to switch port 1 for the data plane (**Sw 1**).

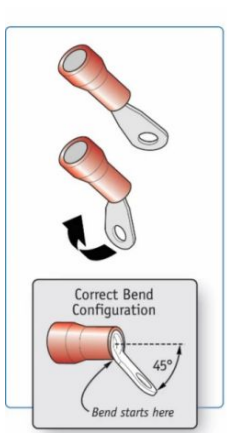


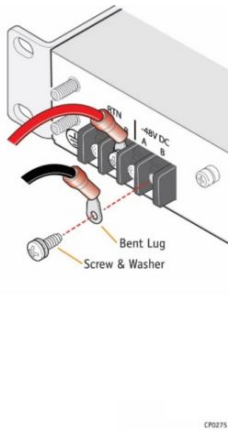
Preparing and connecting the DC power supply cables

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.
⚠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.

Procedure

Step_1	Strip 6 mm [0.236 in] from the end of a black stranded 14 AWG wire (for Molex crimp lug 19131-0023) or 8 mm [0.315 in] from the end of a black stranded 12 AWG wire (for Panduit crimp lug EV10-6RB-Q).
Step_2	Strip 6 mm [0.236 in] from the end of a red stranded 14 AWG wire (for Molex crimp lug 19131-0023) or 8 mm [0.315 in] from the end of a red stranded 12 AWG wire (for Panduit crimp lug EV10-6RB-Q).
Step_3	Insert each wire in a crimp lug. Follow the crimp lug manufacturer's procedure, using the appropriate hand crimp tool as specified in the Application tooling specification sheet of the tool.
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.
Step_9	Insert the crimped black wire in the -48V DC "B" location as shown in the image.
Step_10	Screw the crimp lug in place.
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.
Step_12	The power supply is reverse polarity protected. The unit will power on as soon as external power is applied (green power LED).





> 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:

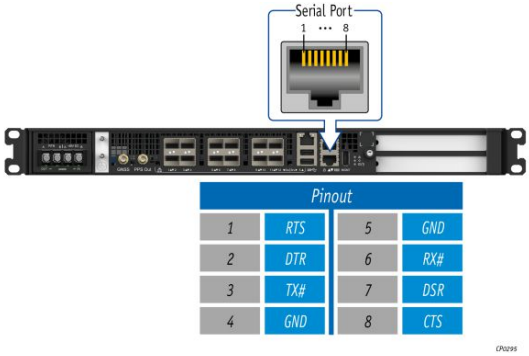
Accessing the UEFI/BIOS using a s erial console (physical connection)

Prerequisites

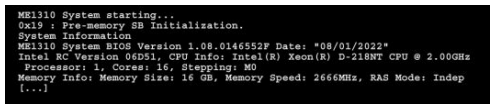
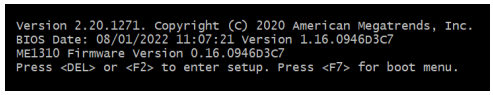
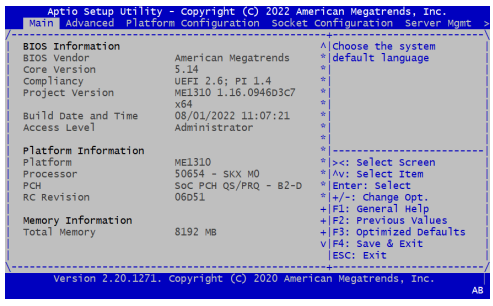
1	A physical connection to the device is required. NOTE: The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the remote computer. • Speed (Baud): 115200 • Data bits: 8 • Stop bits: 1 • Parity: None • Flow Control: None • Recommended emulation mode: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

Relevant sections:
Accessing the UEFI or BIOS
Sending a BREAK signal over a serial connection

Port location

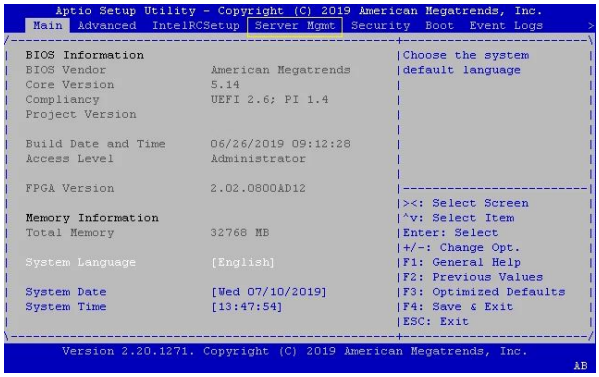
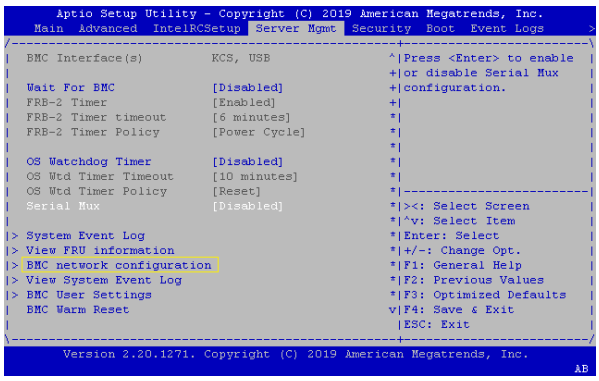
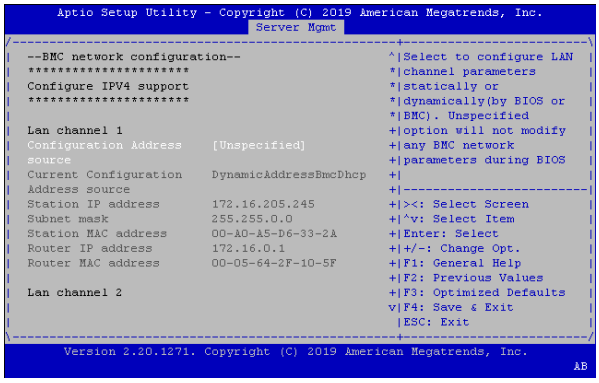


Accessing the UEFI/BIOS setup menu

Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.	
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 hotkey 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.	
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...".	
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.	
Step_5	The UEFI/BIOS setup menu is displayed.	

Accessing the BMC network configuration menu

NOTE: In an ME1310 platform, LAN channel 1 corresponds to port Srv 5, the RJ45 connector.

Step_1	From the UEFI/BIOS menu, navigate to tab **Server Mgmt** .	
Step_2	Select **BMC network configuration** .	
Step_3	The **BMC network configuration** menu is displayed. **NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS .	

Discovering the 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

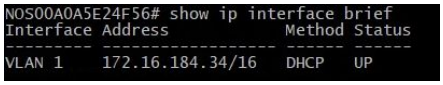
Prerequisites

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 **Enter** followed by ~ .

Step_1	Using an SSH client tool, open an SSH session with the following parameters: • BMC IP address • Port number: 2201 (after login, the BMC will automatically redirect communication to the switch NOS serial console)	
Step_2	Log in the BMC using the appropriate BMC credentials. Upon successful login, press **Enter** to get a response from the switch NOS CLI. If a NOS serial console session is not already active, another set of credentials will be requested. Use the appropriate switch credentials to complete the login into the NOS.	
Step_3	Use the following command to discover the switch NOS IP address. LocalSwitchNOS_OSPrompt:~# **show ip interface brief**	

> 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 Default user names and passwords .

Prerequisites

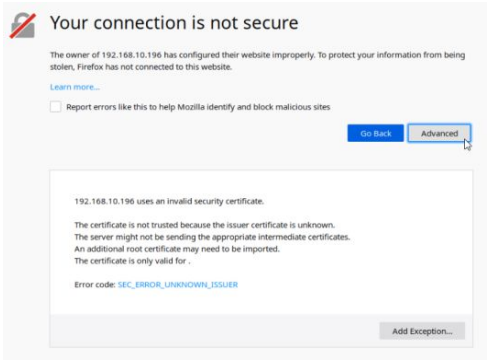
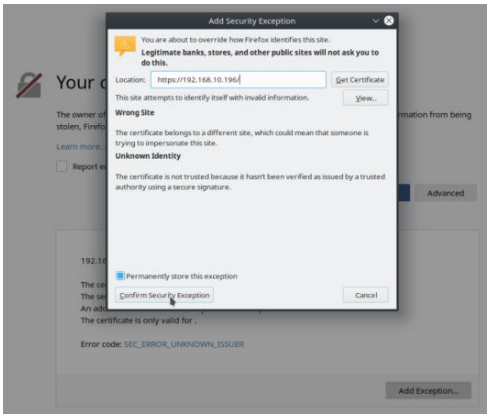
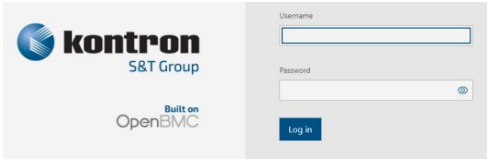
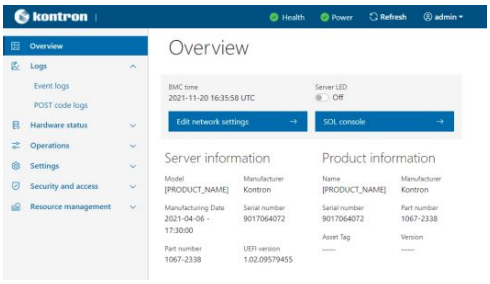
1	The BMC IP address is known.
2	The remote computer has access to the management network subnet.

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.

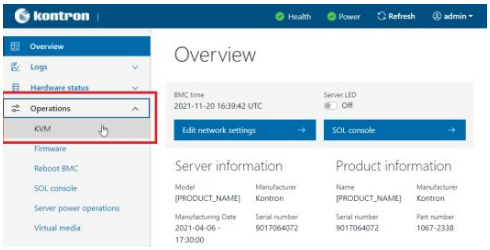
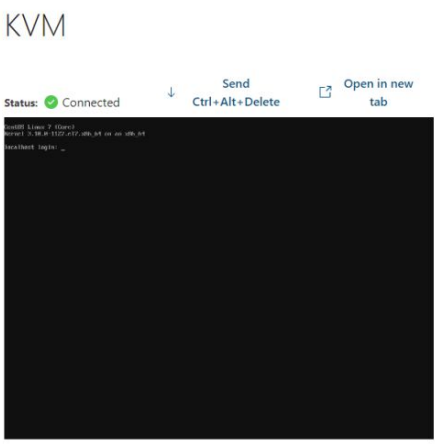
Connecting to the Web UI of the BMC

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.	
Step_3	Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	

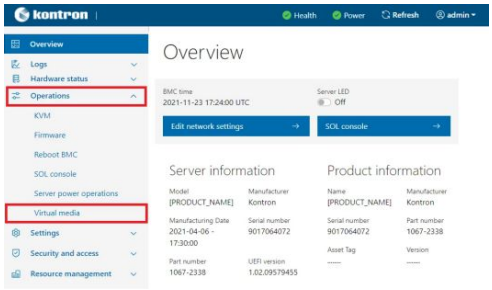
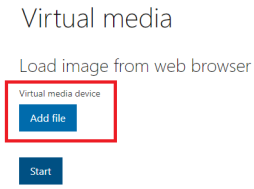
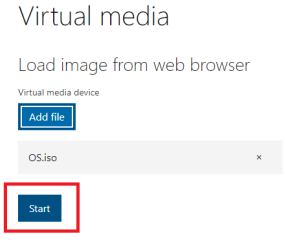
	It is recommended to change the administrator password immediately after accessing the Web UI.

Launching the KVM

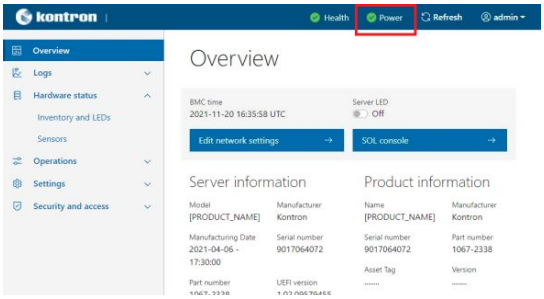
The Web UI allows remote control of the server through a KVM (Keyboard, Video, Mouse) interface.

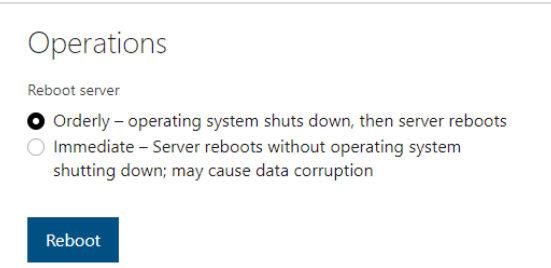
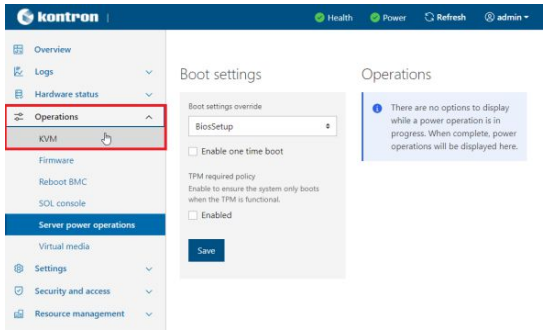
Step_1	From the left-side menu of the BMC Web UI, click on **Operations** and then on **KVM** .	
Step_2	A new browser window opens and displays the virtual server screen.	

Mounting the operating system image via virtual media

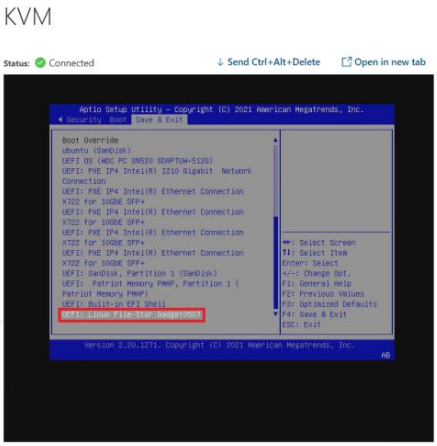
Step_1	From the **Operations** menu, select **Virtual media** .	
Step_2	Click on **Add file** to browse for the ISO file.	
Step_3	Click on **Start** to access virtual media from the OS.	

Accessing the UEFI/BIOS setup menu

Step_1	From the BMC Web UI, click on the **Power** button.	

Step_2	From the **Reboot server** section, select **Orderly** and then click on **Reboot** .	
Step_3	From the **Operations** menu, click on **KVM**.	
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…”.	
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.	

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.	

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

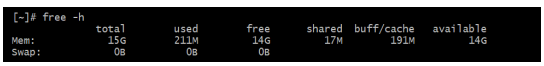
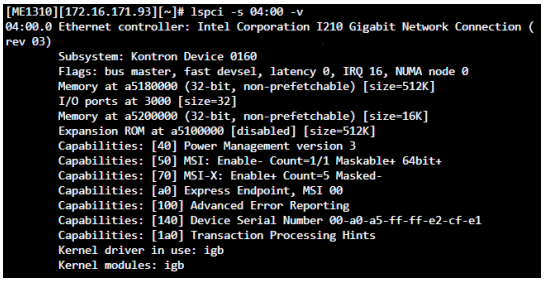
Completing operating system installation

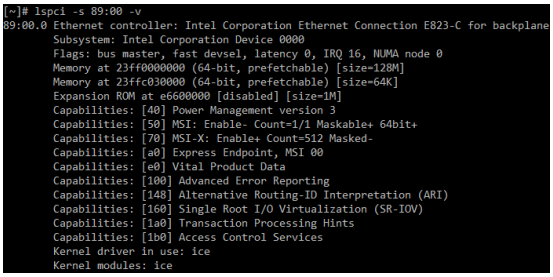
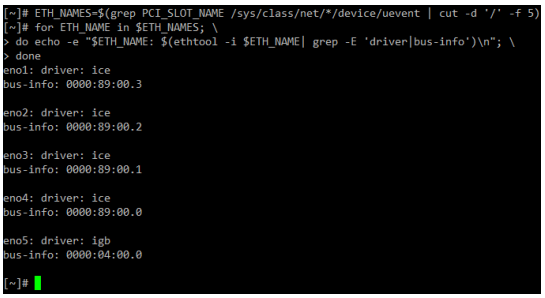
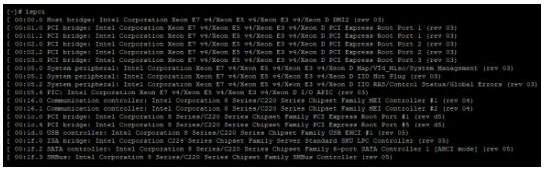
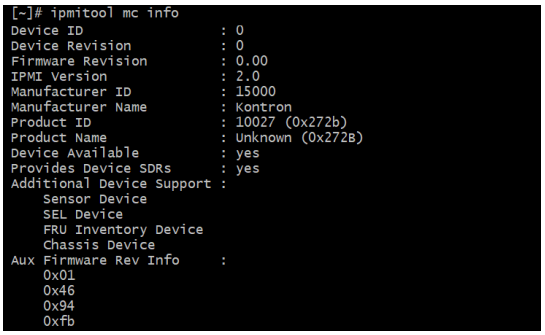
Step_1	Complete the installation by following the on-screen prompts of the specific OS installed.

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 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** **NOTE:** Updating the packages may take a few minutes.	
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**	
Step_5	Verify that all the storage devices are detected. LocalServer_OSPrompt:~# **lsblk**	
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.	

Step_7	Confirm the data plane network interface controllers are loaded by the **ice** driver. LocalServer_OSPrompt:~# **lspci -s 89:00 -v** **NOTE:** You should discover up to four 25GbE NIC.	
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 25GbE 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 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**	
Step_11	Verify communication between the operating system and the BMC. LocalServer_OSPrompt:~# **ipmitool mc info**	

Benchmarking an application

Install your application and proceed with benchmarking.

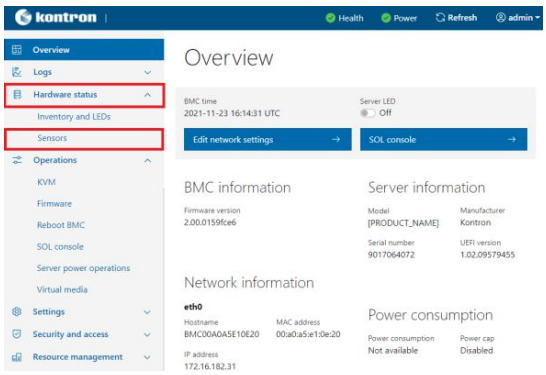
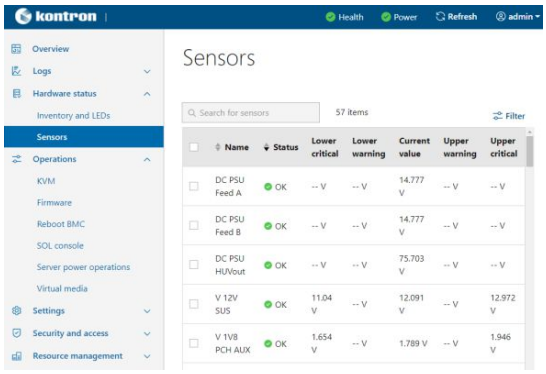
Monitoring platform sensors

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** .	
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.	

Mechanical installation and precautions

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.

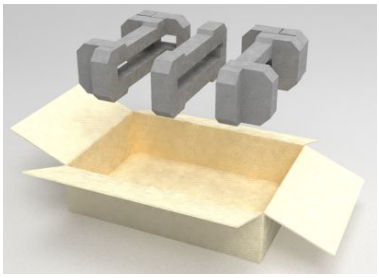
We recommend that you perform all the installation procedures described in the documentation at an ESD workstation. If this is not possible, apply ESD protections such as the following:

- 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

The box includes **one ME1310 multi-access edge computing 1U platform** .



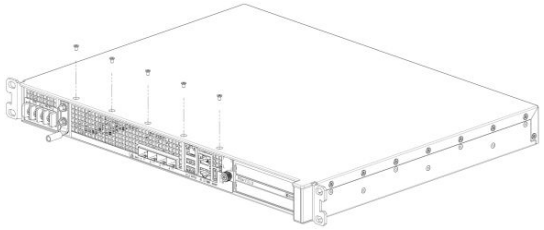
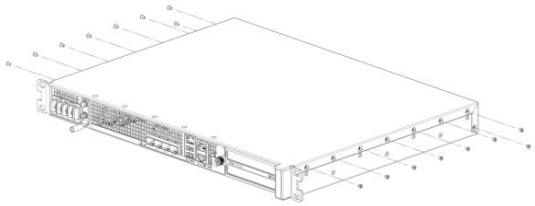
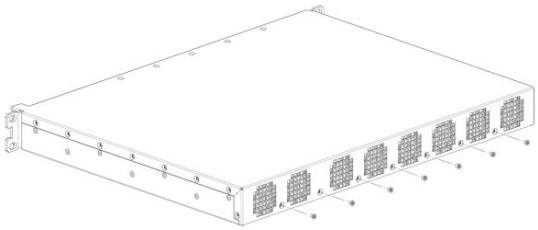
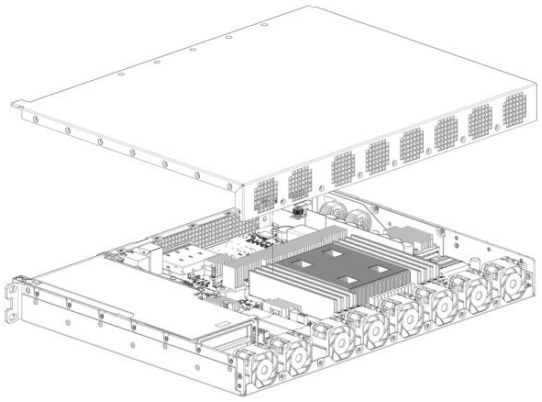
Step_1	Carefully remove the platform from its packaging.
Step_2	Remove the plastic film from the platform. **Failure to do so may affect platform airflow efficiency, thus resulting in poor cooling capabilities.**

Components installation and assembly

Table of contents

	**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 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).

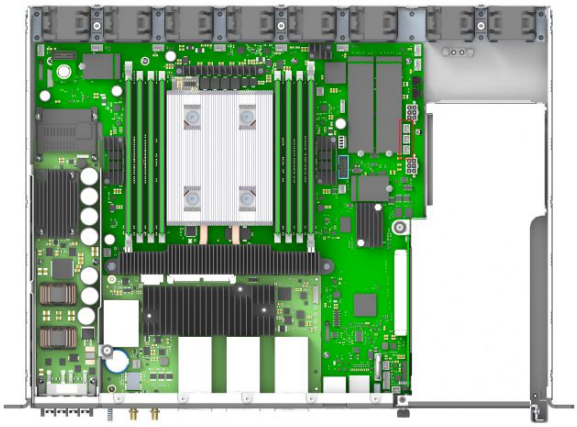
(Optional) Installing a thermal probe for the PCIe add-in card

For the thermal probe part number, refer to Platform, modules and accessories .

(Optional) Locating the thermal probe connection

There are three thermal probe connectors on an ME1310.

Location	Reference designator	Connector
Back	J20	PCIe slot 1
Middle	J21	PCIe slot 2
Front	J23	Chassis



(Optional) Building a thermal probe

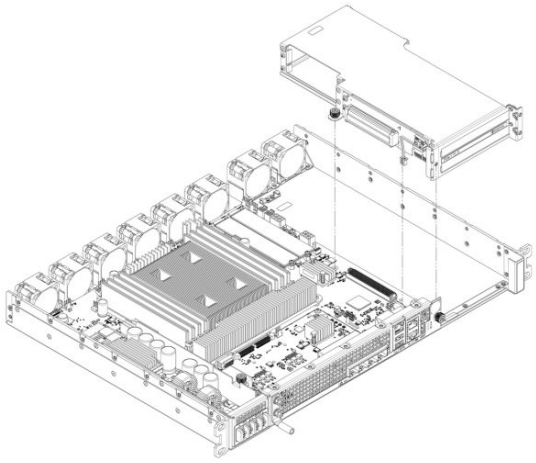
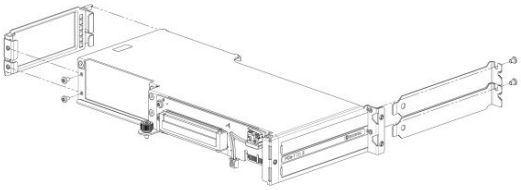
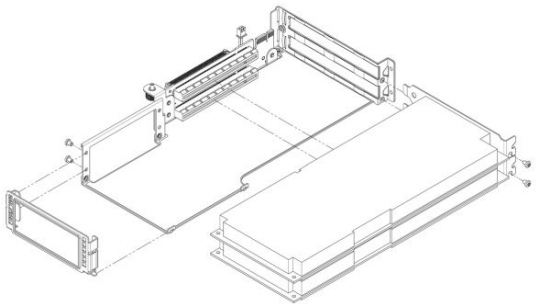
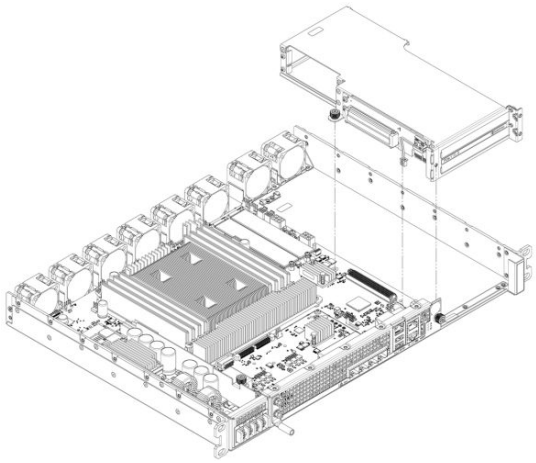
Component	P/N	Description
NTC thermistor	GA10K3A1IA	NTC thermistor 10 Kohm, 3976K Bead
Connector	XHP-2	Connector housing 2.5 mm, 2 position
Pins	SXH-001-P0.6	Socket contact, 22-28 awg, crimp stamped

Step_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.

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 lbs-in torque) . Mount the PCIe rear holder onto the assembly and tighten the M3 screws with a T10 Torx screwdriver (6 lbs-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 lbs-in torque). Connect the intrusion detection switch wire near the front of the chassis.	

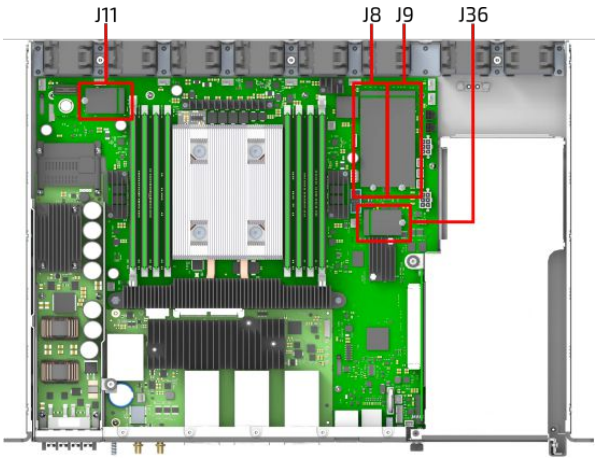
(Optional) Software installation instructions

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

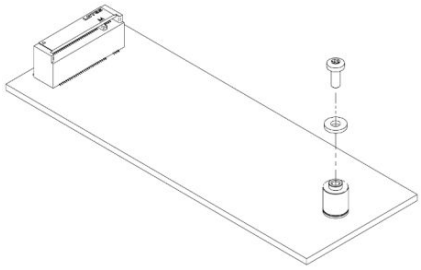
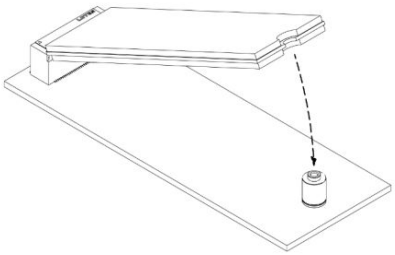
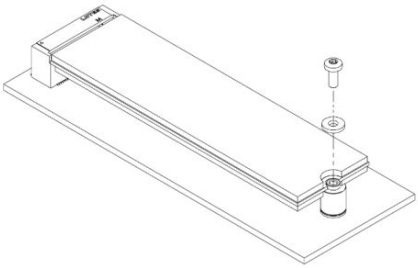
Installing an M.2 storage

Up to four M.2 storage drives can be installed in an ME1310.
For the list of tested M.2 storages, refer to Hardware compatibility list .

Locating the M.2 storage



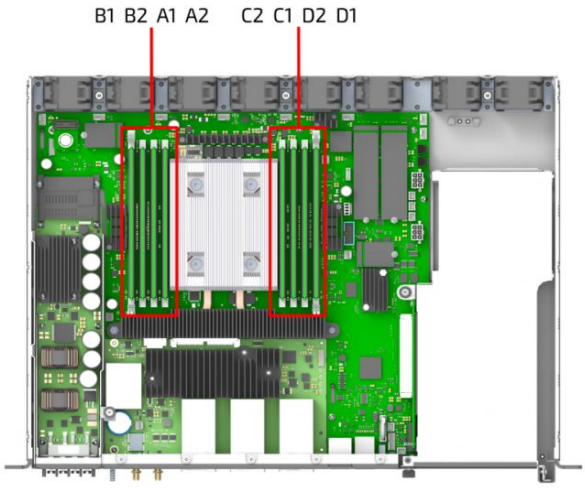
Installing the M.2 storage

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 lbs-in torque) .	

Installing DIMMs

Up to eight DIMMs can be installed in an ME1310.
For the list of tested DIMMs, refer to Hardware compatibility list .

Locating the DIMMs



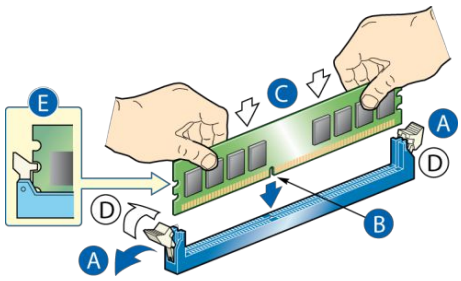
DIMM population guidelines for optimal performance

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, C1 and C2 are on the same channel, and D1 and D2 are on the same channel.
Therefore, do not populate A2, B2, C2 and D2 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 DIMM – populate slot C1.
- For configurations with 2 DIMMs – populate slots A1 and C1.
- For configurations with 4 DIMMs – populate slots A1, B1, C1 and D1
- For configurations with 8 DIMMs – populate all DIMM slots.
- Other DIMM configurations are not recommended, as they may be unbalanced and will produce a less optimal performance.

Installing a DIMM

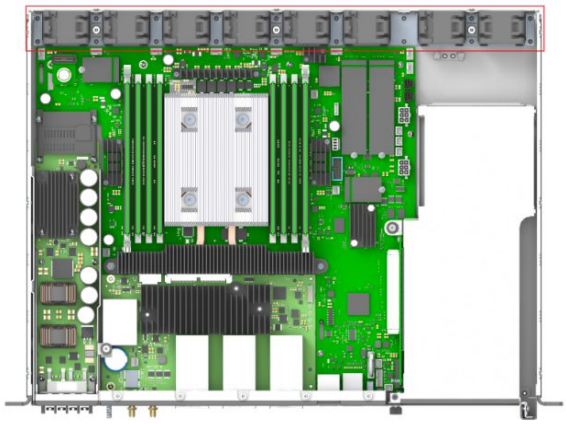
Step_1	Open the levers of the DIMM slot. (A)
Step_2	Note the location of the alignment notch on the DIMM edge. (B)
Step_3	Insert the DIMM, making sure the connector edge of the DIMM aligns correctly with the slot. (E)
Step_4	Using both hands, push down firmly and evenly on both sides of the DIMM until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



Replacing fans

There are eight fans in this platform.

Locating the fans



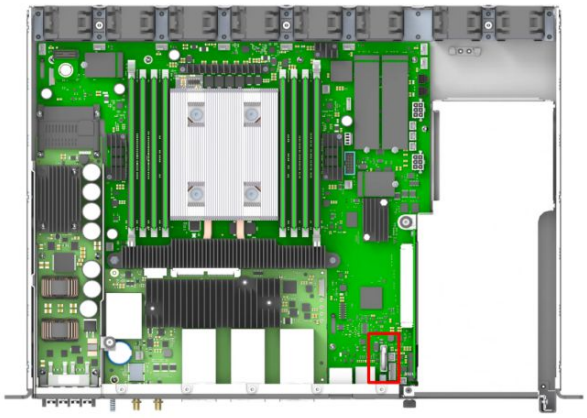
Replacing a fan

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.

Replacing the RTC battery

⚠CAUTION	Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

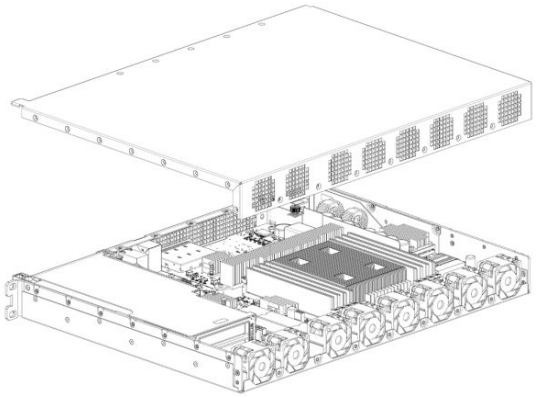
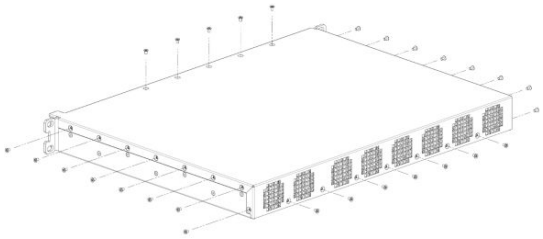
Locating the RTC battery



Replacing the battery

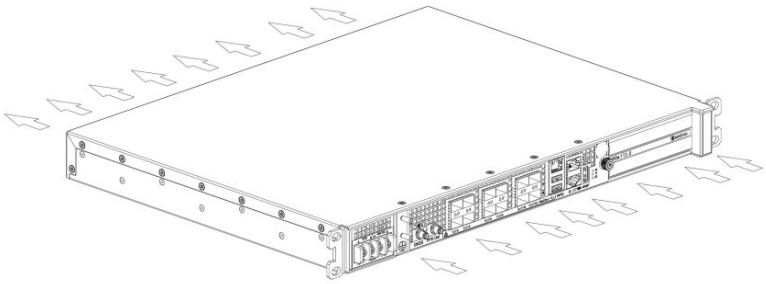
Step_1	A latch pin secures the battery in place. With one hand, gently push the latch to release the battery. While holding the latch, use the other hand to remove the battery.
Step_2	Safely dispose of the battery.
Step_3	With one hand, gently push the latch and insert a new battery with the other hand. Respect the appropriate orientation and polarity.

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

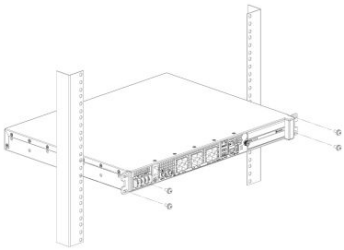
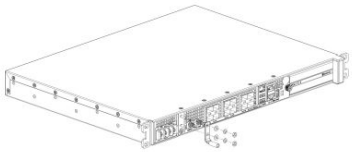
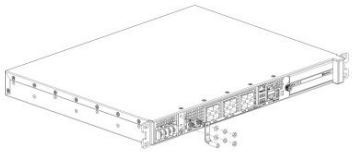
The ME1310 platform features a front to back air flow system. To optimize heat transfer, refer to the Specifications section for the ideal clearances.



Rack installation

Installing an ME1310 pla tform 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).	
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

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

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.
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

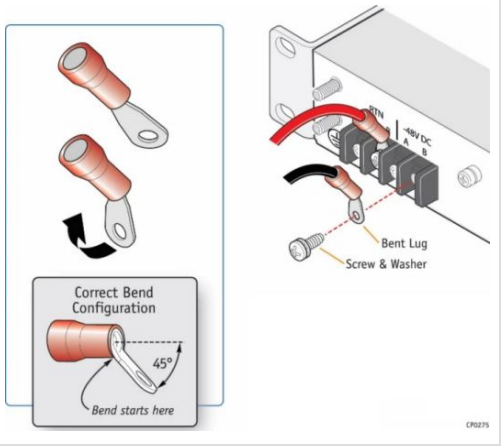
Kontron suggests using crimp lugs (ring or spade crimp lug, straight, isolated, UL94V-0) on the power cables. Connect the appropriate cable to the appropriate polarity.

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 gauge • Panduit insulated ring crimp lugs for 10-12 wire gauge	2 (or 4 for redundancy)	19131-0023 or equivalent	• Molex product catalog • Part details
		EV10-6RB-Q or equivalent	• Panduit product catalog • Part drawing
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 • Panduit Hand Crimp Tool	1	640010100 or equivalent	• Molex product catalog • Application tooling specification sheet
		CT-460 or equivalent	• Panduit product catalog • Application tooling specification sheet

Procedure

Step_1	Strip 6 mm [0.236 in] from the end of a black stranded 14 AWG wire (for Molex crimp lug 19131-0023) or 8 mm [0.315 in] from the end of a black stranded 12 AWG wire (for Panduit crimp lug EV10-6RB-Q).
Step_2	Strip 6 mm [0.236 in] from the end of a red stranded 14 AWG wire (for Molex crimp lug 19131-0023) or 8 mm [0.315 in] from the end of a red stranded 12 AWG wire (for Panduit crimp lug EV10-6RB-Q).
Step_3	Insert each wire in a crimp lug. Follow the crimp lug manufacturer's procedure, using the appropriate hand crimp tool as specified in the Application tooling specification sheet of the tool.
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.
Step_9	Insert the crimped black wire in the -48V DC "B" location as shown in the image.
Step_10	Screw the crimp lug in place.
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.
Step_12	The power supply is reverse polarity protected. The unit will power on as soon as external power is applied (green power LED).



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.

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

Power cord usage guidelines

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

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

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

AC power supply connection

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

For information on grounding, refer to Rack installation .
For information on LED behavior, refer to Platform components .

GNSS input

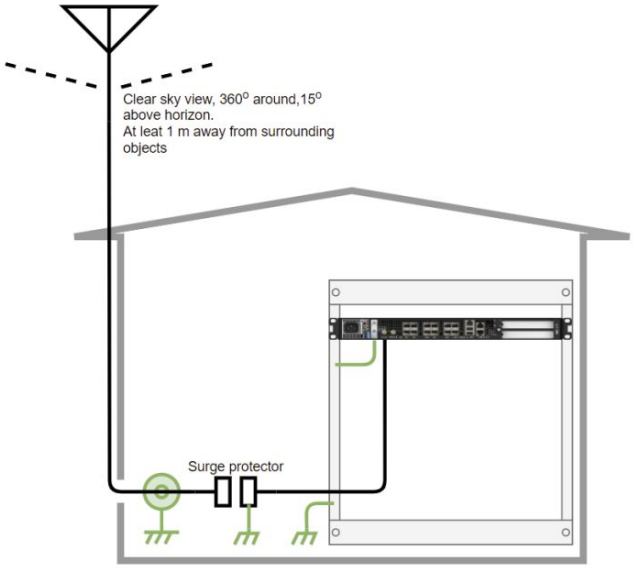
Connecting to an RF splitter

Step_1	Connect a 50-ohm coaxial cable from the splitter to the platform. **NOTE:** The platform 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 platform 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

⚠WARNING	When connecting an external antenna, proper grounding is required and additional surge protection may be required. Always refer to your local electrical code.

	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 platform 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 platform. This cable needs an SMA connection on the platform side.

Accessing platform components

Accessing a BMC

Table of contents

A BMC can be accessed through various methods:

- Using the Web UI – this is the recommended path for first time out-of-the-box system configuration
- Using Redfish
- Using IPMI over LAN (IOL)
- Using IPMI via KCS

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

Accessing a BMC using the Web UI

Prerequisites

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

Relevant sections:

Discovering platform IP addresses

Configuring the BMC networking

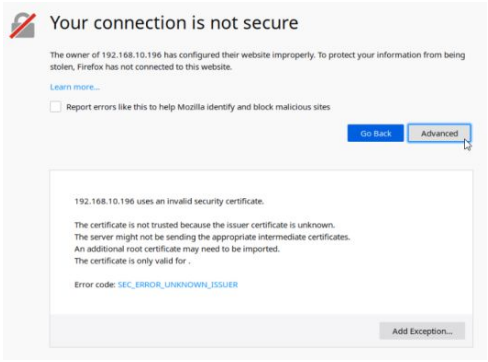
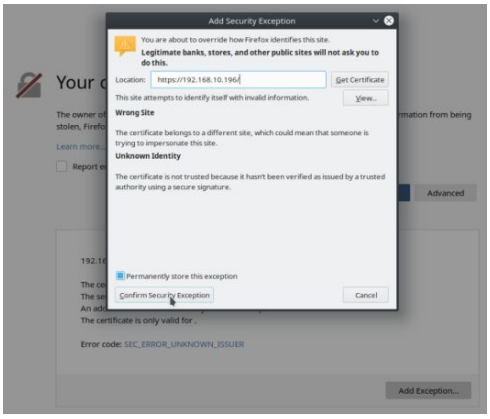
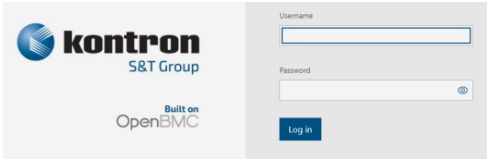
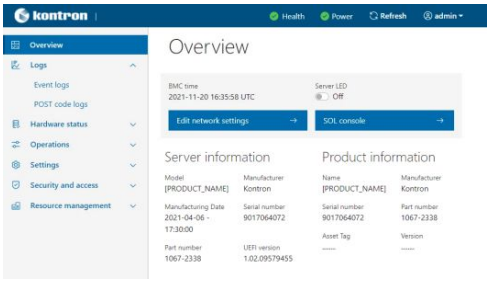
Browser considerations

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

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

Access procedure

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

Step_1	From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC. **NOTE: The HTTPS prefix is mandatory.** *https://[BMC MNGMT_IP]*	
Step_2	Click on **Advanced** in order to s tart the HTTPS self-signed certificate acceptance process . Information on the error message will be displayed.	
Step_3	Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	

Accessing a BMC using Redfish

There are two methods to access the BMC:

- Via an external network connection
- 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.

NOTE: If you are already logged in the BMC Web UI, the URL can be pasted directly in a Web browser to view results. If this is the method chosen, prerequisites 2 and 3 are not required. However, no commands can be executed to change or configure parameters.

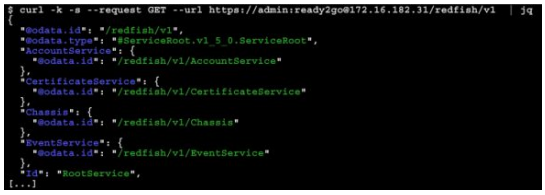
Relevant sections:
Discovering platform IP addresses
Configuring and managing users (if a password needs to be changed)

Creating the Redfish ROOT_URL

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

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 GET --url [ROOT_URL] /redfish/v1/ | jq**	

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 ME1310, this is implemented using a USB-LAN interface. Most modern Linux operating systems should have built-in support for this USB-LAN device.

Prerequisites

1	The IP address of the Redfish host interface is configured.
2	An HTTP client tool is installed on the remote computer.
3	A JSON parsor command-line tool such as **jq** is installed.

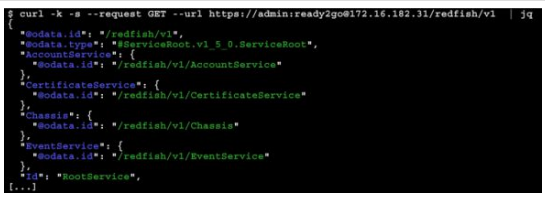
Relevant sections:
Configuring the Redfish host interface
Configuring and managing users (if a password needs to be changed)

Creating the Redfish ROOT_URL to use with the Redfish host interface

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

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 configured Redfish host interface IP address.	https:// [BMC_USERNAME] : [BMC_PASSWORD] @ 169.254.0.17 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 pro cedure

Step_1	Access Redfish. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/ | jq**	

Accessing a BMC using IPMI over LAN (IOL)

Prerequisites

1	The BMC IP address is known.
2	The remote computer has access to the management network subnet.
3	A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

Relevant sections:
Discovering platform IP addresses
Configuring the BMC networking

Access procedure

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

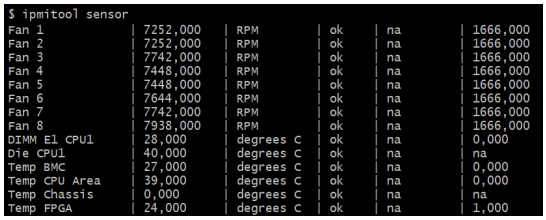
Step_1	From a remote computer that has access to the management network subnet, enter the desired command. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 [IPMI command]**	

Accessing a BMC using IPMI via KCS

Prerequisites

1	An OS is installed.
2	The remote computer has access to the server OS (SSH/RDP/platform serial port).
3	A community version of ipmitool is installed on the local server to enable local monitoring—it is recommended to use ipmitool version 1.8.18.

Access procedure

Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, enter the desired command. LocalServer_OSPrompt:~# **ipmitool [IPMI command]**	

Accessing the operating system of a server

Table of contents

An operating system can be accessed through various methods:

- Using the KVM – this is the recommended path for first time out-of-the-box system configuration
- Using the Web UI Serial over LAN console
- Using Serial over LAN using SSH
- Using IPMI Serial over LAN
- Using SSH/RDP/Customer application protocols
- 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.
3	The remote computer has access to the management network subnet.

Relevant sections:

Accessing a BMC
Discovering platform IP addresses
Platform power management

Browser considerations

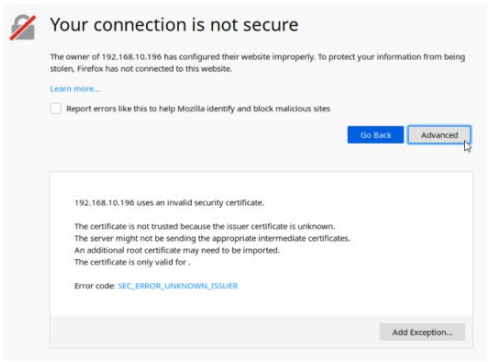
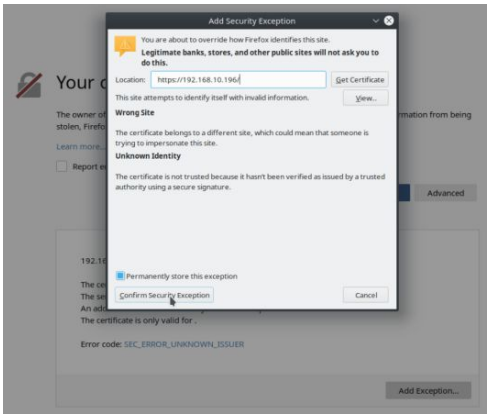
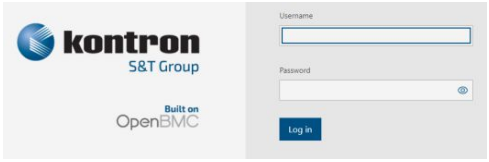
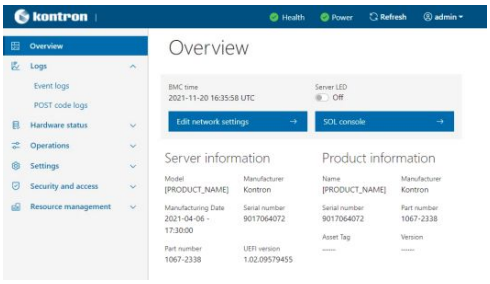
HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self-signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's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

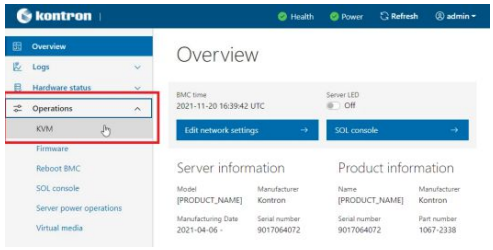
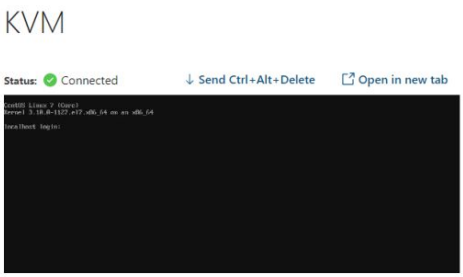
Accessing the BMC of the server for which you want to access the OS

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

Step_1	From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC. **NOTE: The HTTPS prefix is mandatory.** *https://[BMC MNGMT_IP]*	
Step_2	Click on **Advanced** in order to s tart the HTTPS self-signed certificate acceptance process . Information on the error message will be displayed.	
Step_3	Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	

Launching the KVM

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

Step_1	From the BMC Web UI, click on the **Operations** menu and then on the **KVM** button.	
Step_2	The OS screen should be displayed.	

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

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.
4	Redirection to the serial port is configured in the OS. **NOTE:** If the OS was installed by Kontron, console redirection is enabled by default.

Relevant sections:
Accessing a BMC
Discovering platform IP addresses
Platform power management

Browser considerations

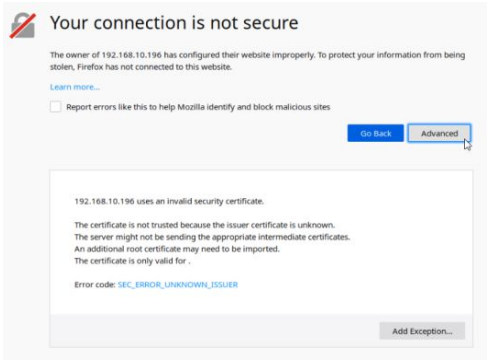
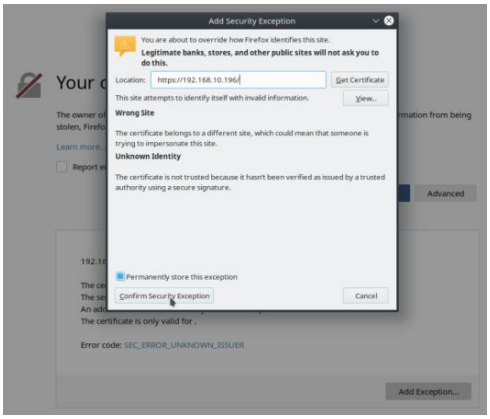
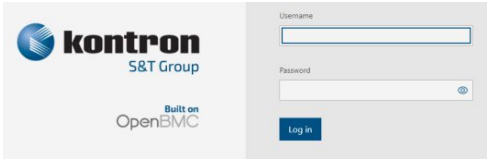
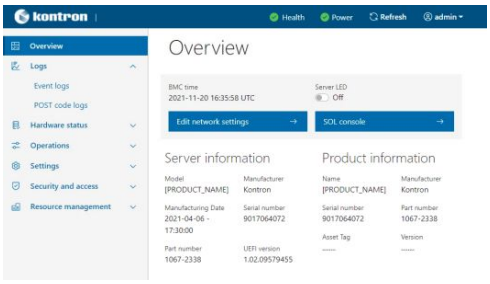
HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self-signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's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

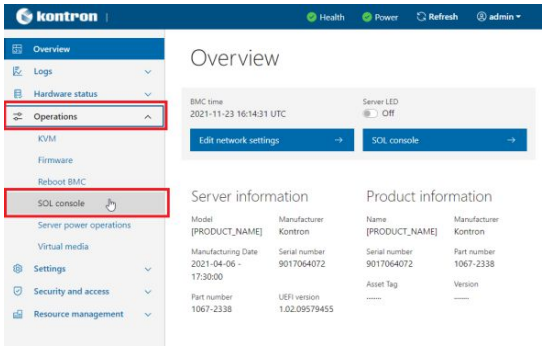
Access procedure

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 Default user names and passwords .

Step_1	From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC. **NOTE: The HTTPS prefix is mandatory.** *https://[BMC MNGMT_IP]*	
Step_2	Click on **Advanced** in order to s tart the HTTPS self-signed certificate acceptance process . Information on the error message will be displayed.	
Step_3	Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	

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.	
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 .	

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

Accessing an OS using Serial over SSH

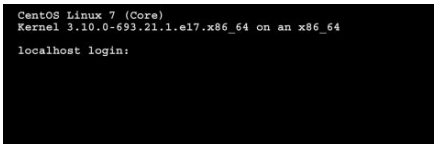
Prerequisites

1	An OS is installed.
2	The BMC IP address is known.
3	The remote computer has access to the management network subnet.
4	An SSH client tool is installed on the remote computer. NOTE: PuTTY is recommended for Windows environments and SSH is recommended for Linux environments.
5	Redirection to the serial port is configured in the OS. NOTE: If the OS was installed by Kontron, console redirection is enabled by default.

Relevant sections:
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 Default user names and passwords .

Step_1	Using an SSH client tool, open an SSH session with the following parameters: • BMC IP address • Server port number: 2200	
Step_2	Log in the BMC using the appropriate credentials. Upon successful login, press **Enter** to get a response from the OS serial console.	

Accessing an OS using IPMI Serial over LAN

Prerequisites

1	An OS is installed.
2	The BMC IP address is known.
3	The remote computer has access to the management network subnet.
4	A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

Relevant sections:
Discovering platform IP addresses
Platform power management

Access procedure

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

Step_1	From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name]-P [IPMI password] -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**	
Step_3	The OS start screen will be displayed.	

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

Accessing an OS using 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:
Platform power management

Access procedure

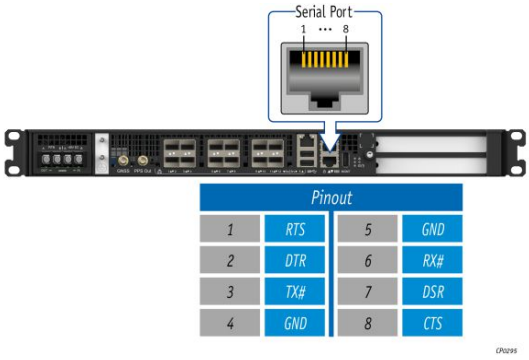
Step_1	Using the OS IP address, proceed with your preferred remote access method.

Accessing an OS using a serial console (physical connection)

Prerequisites

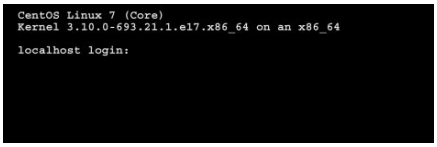
1	An OS is installed.
2	A physical connection to the device is required. **NOTE:** The serial console port is compatible with Cisco 72-3383-01 cable.
3	A serial console tool is installed on the remote computer. • Speed (Baud): 115200 • Data bits: 8 • Stop bits: 1 • Parity: None • Flow Control: None •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



Access procedure

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

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.	

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

Accessing the UEFI or BIOS

Table of contents

UEFI/BIOS can be accessed through various methods :

- Serial over LAN (SOL) using the Web UI – this is the recommended path for first time out-of-the-box system configuration
- KVM
- Serial over SSH
- Serial over LAN (SOL) using IPMI
- Redfish (this feature is under development)
- Serial console (physical connection)

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

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

Relevant section:
Discovering platform IP addresses

Browser considerations

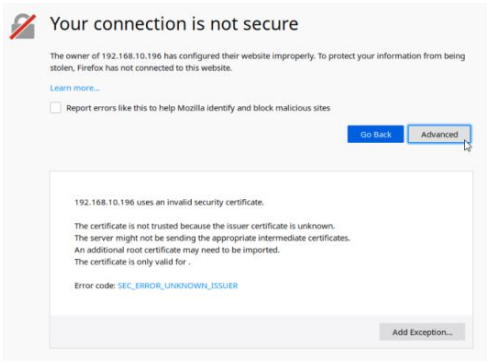
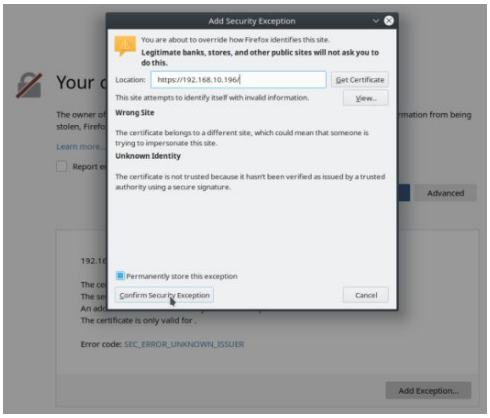
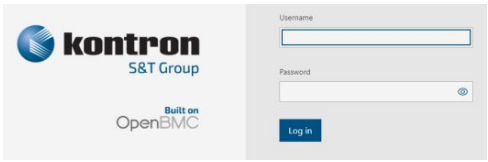
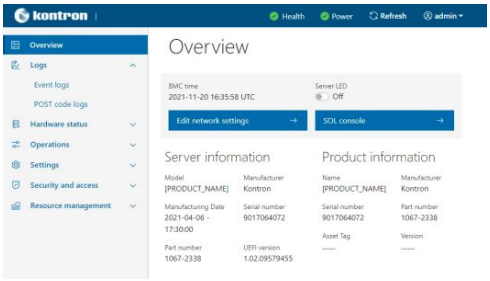
HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self-signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's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

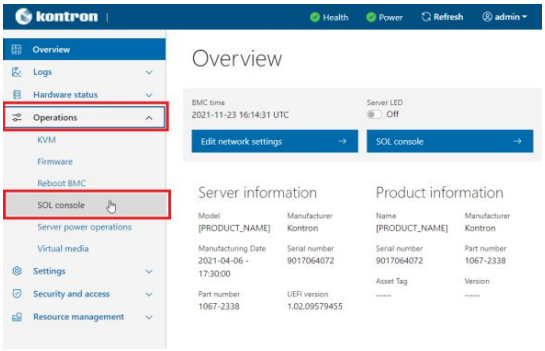
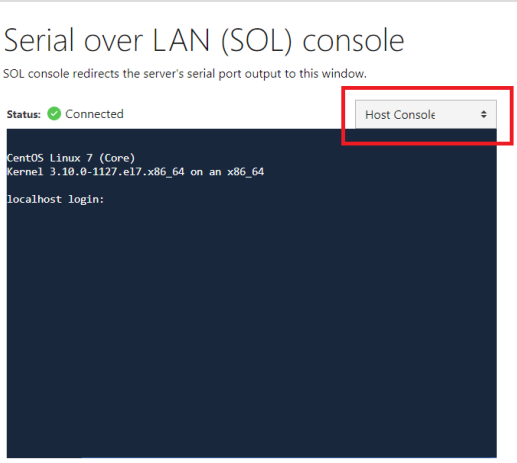
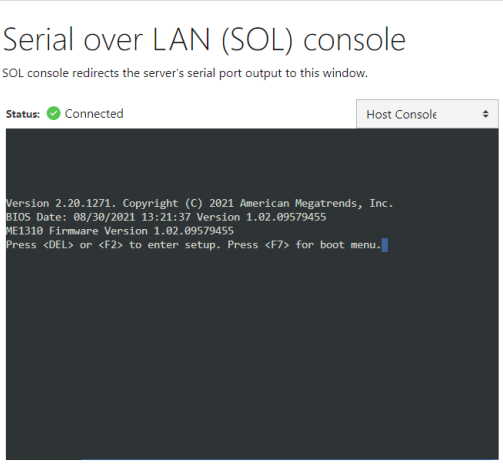
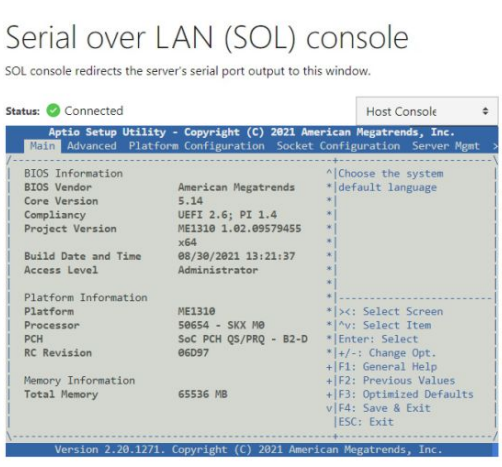
Access procedure

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.** *https://[BMC MNGMT_IP]*	
Step_2	Click on **Advanced** in order to s tart the HTTPS self-signed certificate acceptance process . Information on the error message will be displayed.	
Step_3	Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	

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 the **SOL console** button.	
Step_2	Press an arrow on the keyboard to refresh the console. The OS screen should be displayed. **NOTE:** If the screen is not displayed, make sure that the dropdown menu is set to **Host Console** .	
Step_3	If the system is already powered on, perform a server reset. Otherwise, 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. **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…"	
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.	

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.

Relevant section:
Discovering platform IP addresses

Browser considerations

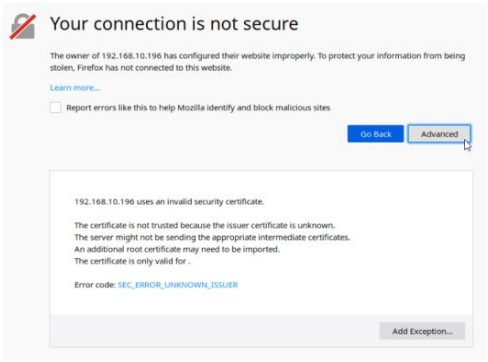
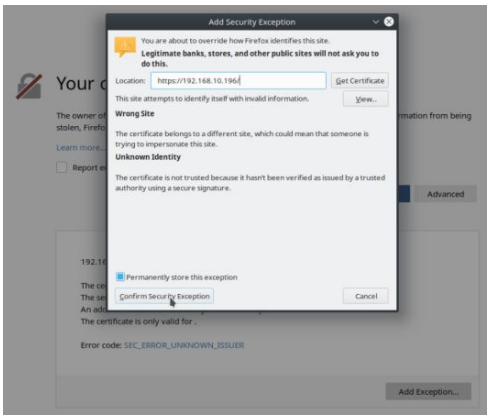
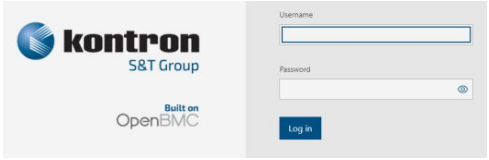
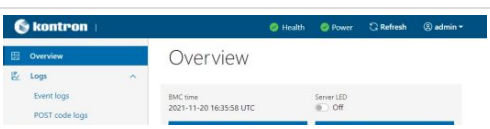
HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self-signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's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

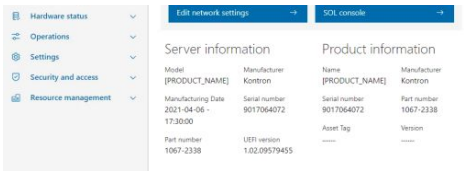
NOTE: The procedure may vary depending on the browser used. Examples provided use Firefox.

Access procedure

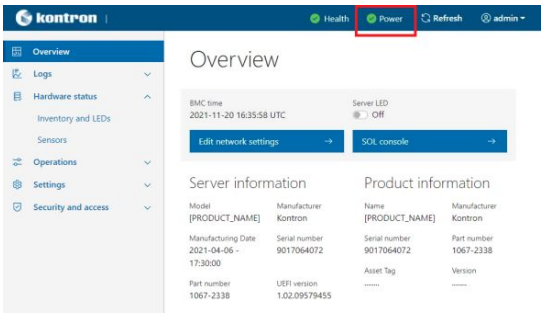
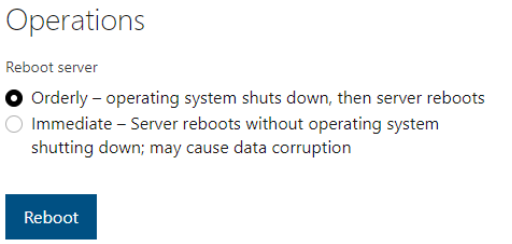
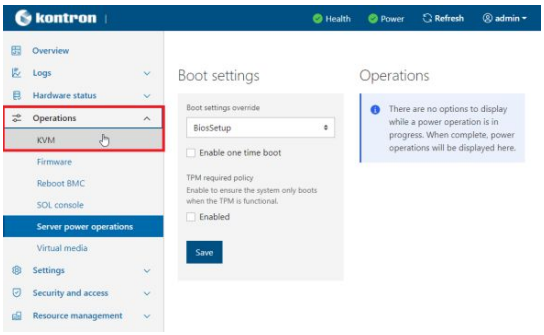
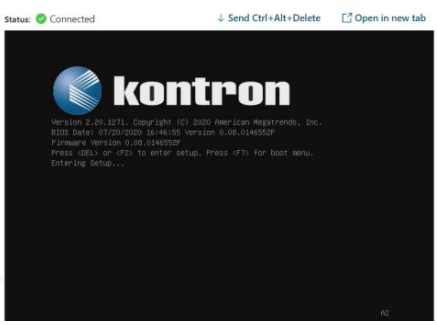
To obtain the list of default user names and passwords, refer to Default user names and passwords .
NOTE: The KVM sometimes loses connection. Simply refresh the Web browser page to establish the connection.

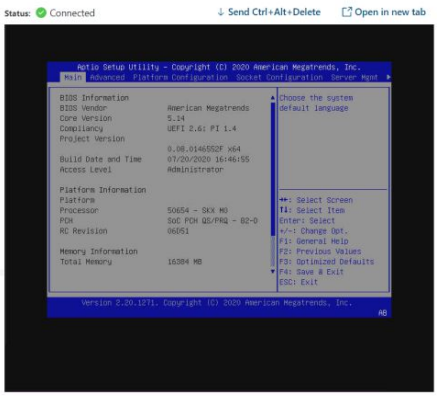
Accessing the BMC Web UI

Step_1	From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC. **NOTE: The HTTPS prefix is mandatory.** *https://[BMC MNGMT_IP]*	
Step_2	Click on **Advanced** in order to s tart the HTTPS self-signed certificate acceptance process . Information on the error message will be displayed.	
Step_3	Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	



Accessing the UEFI/BIOS setup menu using the KVM

Step_1	From the BMC Web UI, click on the **Power** button.	
Step_2	From the **Reboot server** section, select **Orderly** and then click on **Reboot** .	
Step_3	From the **Operations** menu, click on **KVM**.	
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…”.	
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.	KVM 

Accessing the UEFI or BIOS using Serial over SSH

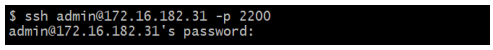
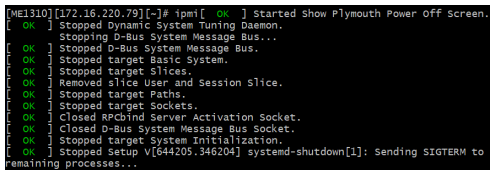
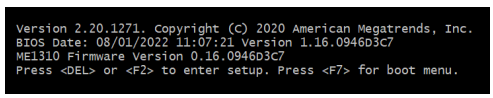
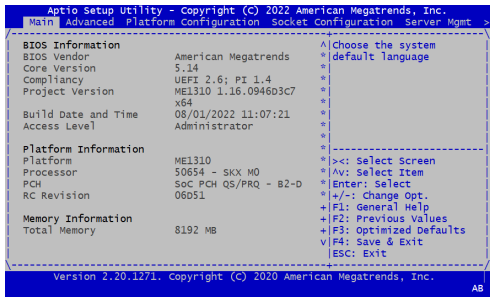
Prerequisites

1	The BMC IP address is known.
2	The remote computer has access to the management network subnet.
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 sections:
Discovering platform IP addresses
Common software installation
Accessing a BMC
Default user names and passwords

Access procedure

NOTE: When using Serial over SSH, to quit the session press **Enter** followed by ~ .

Step_1	Using an SSH client tool, open an SSH session with the following parameters: • BMC IP address • BMC username and password. • Server port number: 2200 Once the password is entered, press on the **Enter** key to generate a response from the server software currently running .	
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.	
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.	
Step_4	The UEFI/BIOS setup menu should be displayed.	

Accessing the UEFI or BIOS using Serial over LAN using IPMI

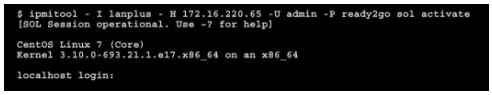
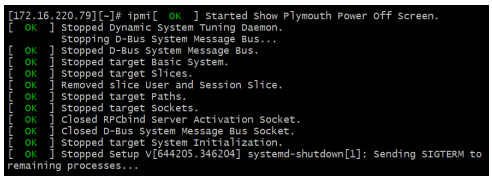
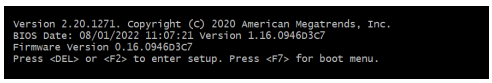
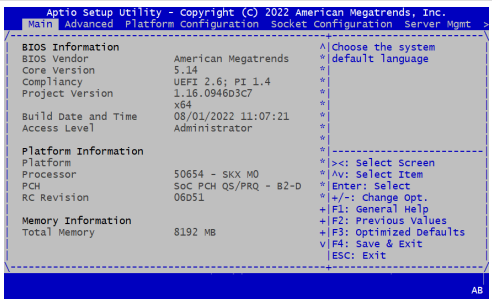
Prerequisites

1	An OS is installed.
2	The BMC IP address is known.
3	The remote computer has access to the management network subnet.
4	A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

Relevant sections:
Discovering platform IP addresses
Common software installation

Access procedure

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

Step_1	From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -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.	
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**	
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.	
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.	
Step_6	The UEFI/BIOS setup menu should be displayed.	

Accessing the UEFI or BIOS using Redfish

This feature is under development.

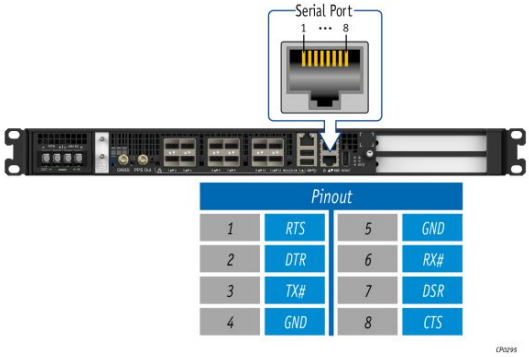
Accessing the UEFI or BIOS using a serial console through a physical connection

Prerequisites

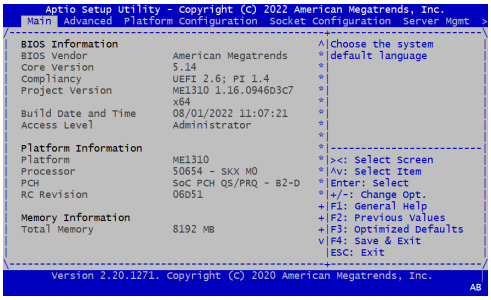
1	A physical connection to the device is required. NOTE: The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the remote computer. • Speed (Baud): 115200 • Data bits: 8 • Stop bits: 1 • Parity: None • Flow Control: None • Recommended emulation mode: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

Relevant sections:
Common software installation
Sending a BREAK signal over a serial connection

Port location



Access procedure

Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.	
Step_2	Perform a server reset 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 hotkey 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.	
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...".	
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.	
Step_5	The UEFI/BIOS setup menu is displayed.	

Accessing the switch NOS

Table of contents

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 the BMC Web UI SOL console
- Using Serial over SSH from a remote computer
- Using SSH from a remote computer
- Using SSH from the integrated server

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 NOS IP addresses is known.
2	The remote computer has access to the switch NOS network subnet.

Relevant section:
Discovering platform IP addresses

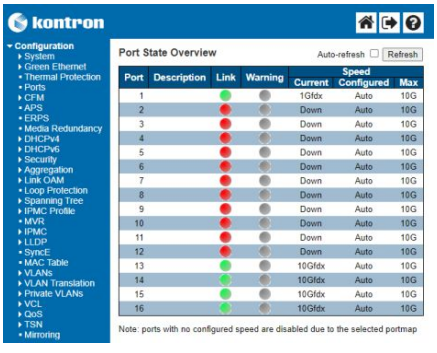
Browser considerations

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.

Step_1	From a remote computer that has access to the switch NOS network, open a browser window and enter the IP address discovered for the switch NOS. *http://[SWITCH_NOS_IP]*	

Accessing the switch NOS CLI using the 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:
Accessing a BMC
Discovering platform IP addresses
Platform power management

Browser considerations

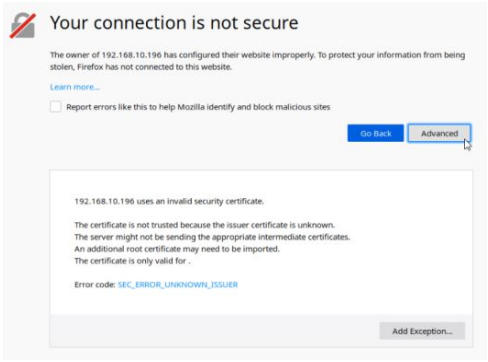
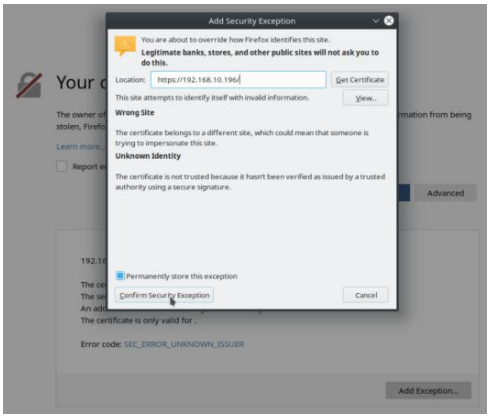
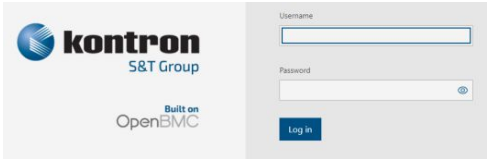
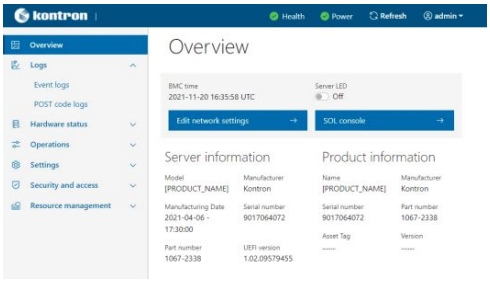
HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self-signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's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

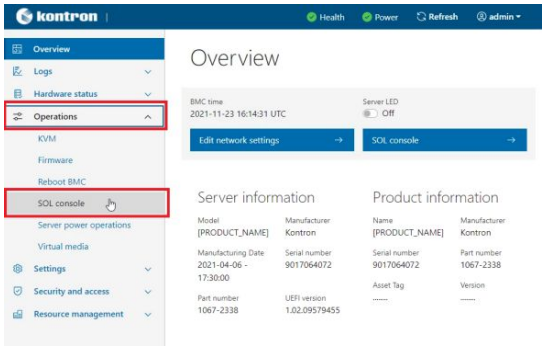
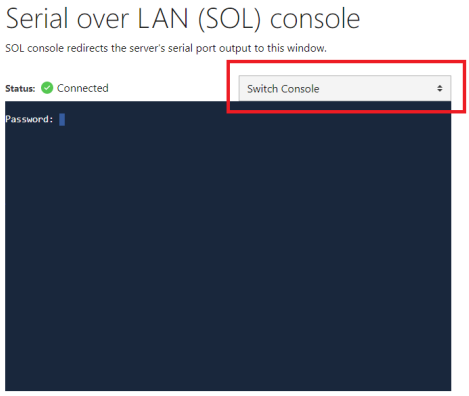
Access procedure

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 Default user names and passwords .

Step_1	From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC. **NOTE: The HTTPS prefix is mandatory.** *https://[BMC MNGMT_IP]*	
Step_2	Click on **Advanced** in order to s tart the HTTPS self-signed certificate acceptance process . Information on the error message will be displayed.	
Step_3	Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	

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.	
Step_2	Change the dropdown menu value to **Switch Console** .	
Step_3	The NOS screen should be displayed.	

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

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

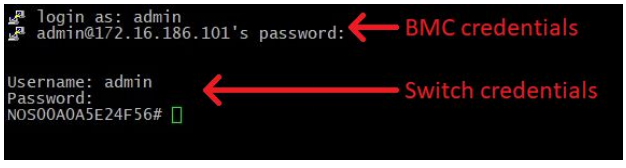
Prerequisites

1	The BMC IP address is known.
2	The remote computer has access to the management network subnet.
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 Default user names and passwords .
NOTE: When using Serial over SSH, to quit the session press **Enter** followed by ~ .

Step_1	Using an SSH client tool, open an SSH session with the following parameters: • BMC IP address • Port number: 2201 (After login, the BMC will automatically redirect communication to the switch NOS serial console)	
Step_2	Log in the BMC using the appropriate credentials for it. Upon successful login, press **Enter** to get a response from the switch NOS CLI. If a NOS serial console session is not already active, another set of credentials will then be requested. Use the appropriate credentials to complete login to the NOS.	

Accessing the switch NOS CLI using SSH from a remote computer

Prerequisites

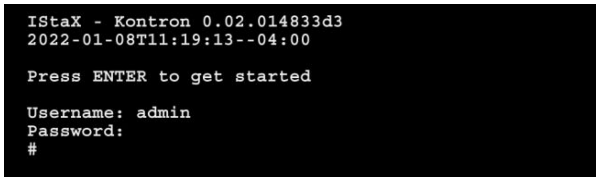
1	The network switch NOS IP address is known.
2	The remote computer has access to the switch NOS network subnet.
3	An SSH client tool is installed on the remote computer. **NOTE:** PuTTY is recommended for Windows environments and SSH is recommended for Linux environments.

Relevant section:

Discovering platform IP addresses

Access procedure

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

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.	

Accessing the switch NOS CLI using SSH from the integrated server

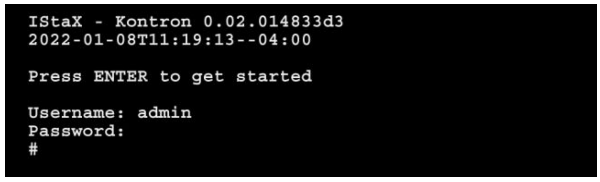
Prerequisites

1	An OS is installed on the integrated server.
2	The remote computer has access to the integrated server OS.
3	One of the switch NOS IP addresses is known.
4	The integrated server has access to the switch NOS 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.

Relevant 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 Default user names and passwords .

Step_1	Access the integrated server operating system using the preferred 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.	

Discovering platform IP addresses

Table of contents

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 DHCP Dynamic DNS update
- Using the UEFI/BIOS via a serial console (physical connection) – device with no OS installed and no known IP address
- Using the DHCP server logs

Discovering the platform BMC IP address with DHCP Dynamic DNS update

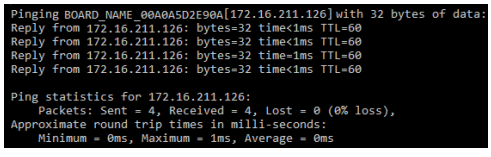
Prerequisites

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

Relevant section:
MAC addresses (to find the first assigned BMC MAC address)

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. Refer to section MAC addresses to determine those specific to a platform.
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	

Discovering the platform BMC IP address using the UEFI or BIOS

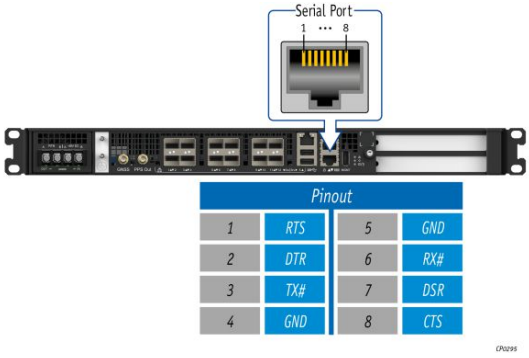
Accessing the UEFI/BIOS using a s erial console (physical connection)

Prerequisites

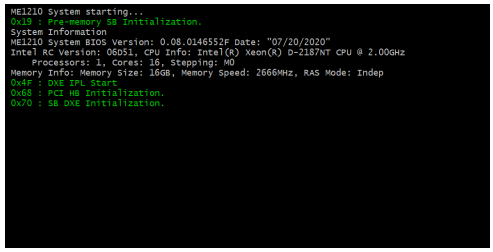
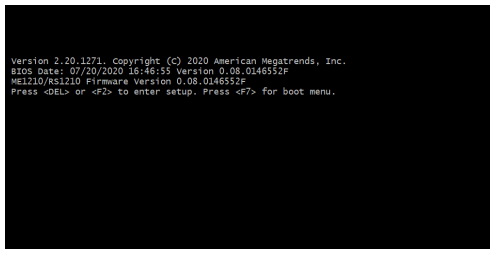
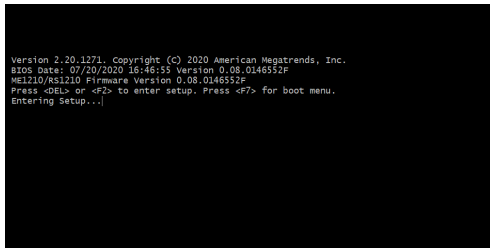
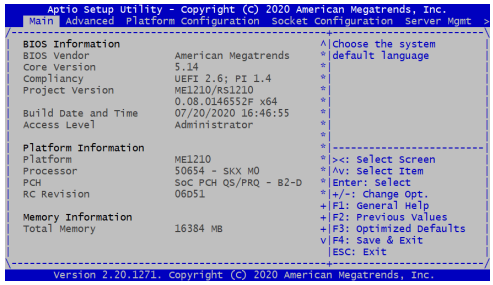
1	A physical connection to the device is required. **NOTE:** The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the remote computer. • Speed (Baud): 115200 • Data bits: 8 • Stop bits: 1 • Parity: None • Flow Control: None • Recommended emulation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

Relevant section:
Sending a BREAK signal over a serial connection

Port location



Accessing the UEFI/BIOS setup menu

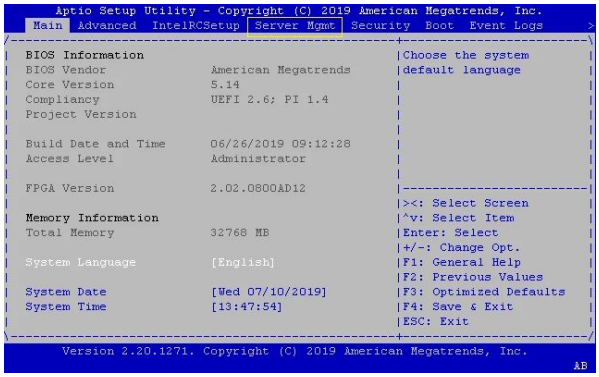
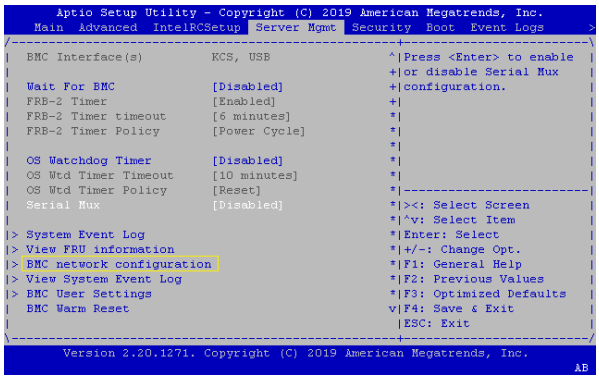
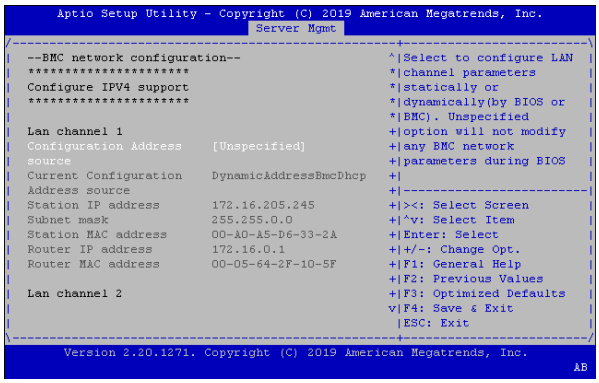
Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.	
Step_2	Perform a server reset using one of the following options: • If the server is currently running an installed 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.	
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...".	
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.	
Step_5	The UEFI/BIOS setup menu is displayed.	

Accessing the BMC network configuration menu

In a 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 → switch port 16 *

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

Step_1	From the UEFI/BIOS menu, navigate to tab **Server Mgmt** .	
Step_2	Select **BMC network configuration** .	
Step_3	The **BMC network configuration** menu is displayed. **NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS .	

Discovering the platform BMC IP address using DHCP server logs

Prerequisites

1	Access to the DHCP server logs is required.
2	The MAC address is known for the BMC interface connected to the network for which the IP address is required.

Relevant section:
MAC addresses (to find the first assigned BMC MAC address)

Procedure

DHCP IP assignment is specific to the network infrastructure to which the platform is being integrated. The assistance of the network administrator may therefore be necessary to obtain the IP address of the device (e.g., BMC, switch NOS, server OS).
If you have the MAC address of the device, you can search the DHCP server logs to determine the IP address assigned to this specific device. Refer to section MAC addresses to determine those specific to a platform.
Various DHCP server services may offer other search capabilities. Please consult the network administrator or the DHCP server documentation. The following example illustrates a command prompt method for use with a Linux based DHCP server. This may need to be adjusted to reflect a specific DHCP infrastructure (this action can generally also be done through a DHCP server Web interface).

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

Variable	Description
00:a0:a5:d2:e9:0a	MAC address discovered for the device (refer to section MAC addresses)
ens192	Linux DHCP server network interface name
172.16.211.126	IP address assigned to the device 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:

- Using DHCP Dynamic DNS update
- Using the switch NOS serial console CLI
- Using the DHCP server logs

Discovering the switch NOS IP address with DHCP Dynamic DNS update

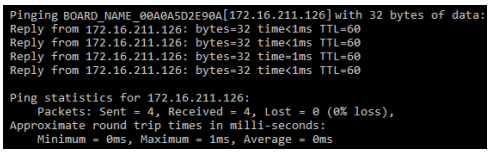
Prerequisites

1	A DHCP server with active Dynamic DNS update feature is available.
2	A remote computer configured with the same DNS information is available.
3	The remote computer has access to the switch NOS network subnet.
4	The first assigned MAC address of the switch NOS is known.

Relevant section:
MAC addresses (to find the first assigned switch NOS MAC address)

Procedure

When requesting a DHCP lease, the platform switch NOS 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 "NOS" prefix and the first switch NOS MAC address. Refer to section MAC addresses to determine those specific to a platform.
For example, if we use the first switch NOS MAC address (**00:a0:a5:d2:e9:0a**), the host name would be: **NOS 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.

Step_1	Ping the host name. RemoteComputer_OSPrompt:~$ **ping NOS00A0A5D2E90A**	

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

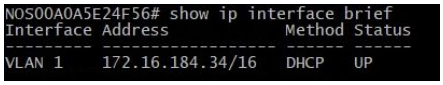
Prerequisites

1	The BMC IP address is known.
2	The remote computer has access to the management 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 sections:
Default user names and passwords
Accessing the switch NOS

Procedure

NOTE: When using Serial over SSH, to quit the session press **Enter** followed by **~** .

Step_1	Using an SSH client tool, open an SSH session with the following parameters: • BMC IP address • Port number: 2201 (after login, the BMC will automatically redirect communication to the switch NOS serial console)	
Step_2	Log in the BMC using the appropriate BMC credentials. Upon successful login, press **Enter** to get a response from the switch NOS CLI. If a NOS serial console session is not already active, another set of credentials will be requested. Use the appropriate switch credentials to complete the login into the NOS.	
Step_3	Use the following command to discover the switch NOS IP address. LocalSwitchNOS_OSPrompt:~# **show ip interface brief**	

Discovering the switch NOS IP address using DHCP server logs

Prerequisites

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

Relevant section:
MAC addresses (to find the first assigned switch NOS MAC address)

Procedure

DHCP IP assignment is specific to the network infrastructure to which the platform is being integrated. The assistance of the network administrator may therefore be necessary to obtain the IP address of the device (e.g., BMC, switch NOS, server OS).
If you have the MAC address of the device, you can search the DHCP server logs to determine the IP address assigned to this specific device. Refer to section MAC addresses to determine those specific to a platform.
Various DHCP server services may offer other search capabilities. Please consult the network administrator or the DHCP server documentation. The following example illustrates a command prompt method for use with a Linux based DHCP server. This may need to be adjusted to reflect a specific DHCP infrastructure (this action can generally also be done through a DHCP server Web interface).

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

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

Default user names and passwords

Table of contents

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

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

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.

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

Installing an operating system on a server

Table of contents

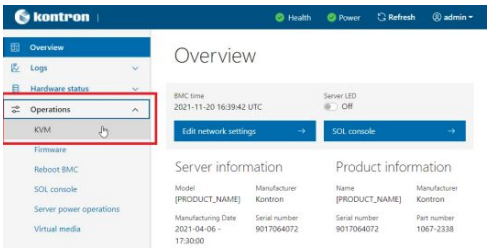
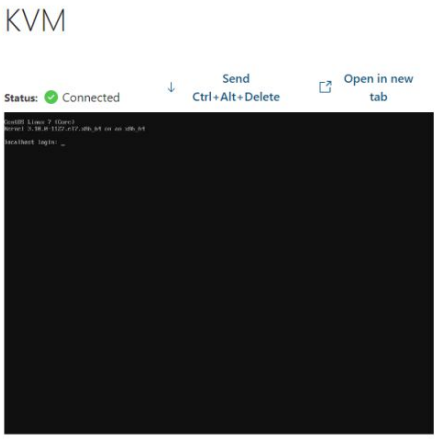
The operating system can be installed using the following methods :

- The KVM
- PXE (Boot from LAN)
- A USB storage device

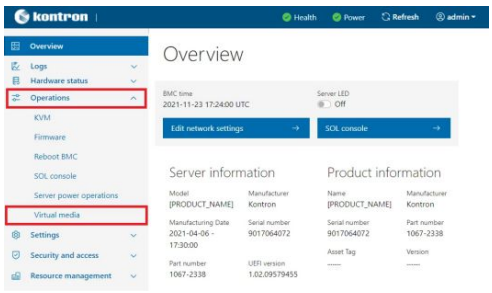
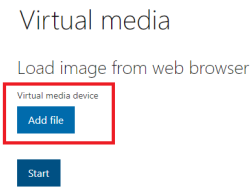
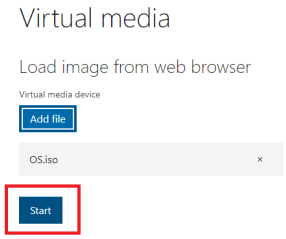
Installing an OS on a server using the KVM

Relevant section:
Accessing a BMC using the Web UI

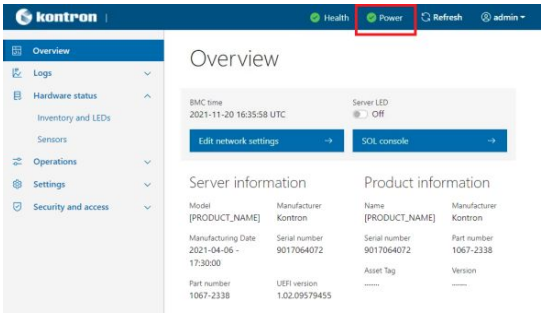
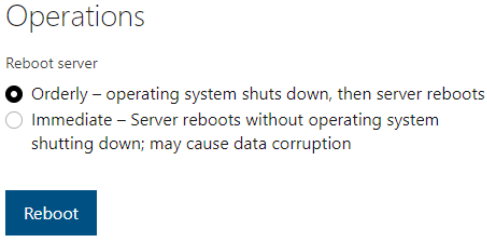
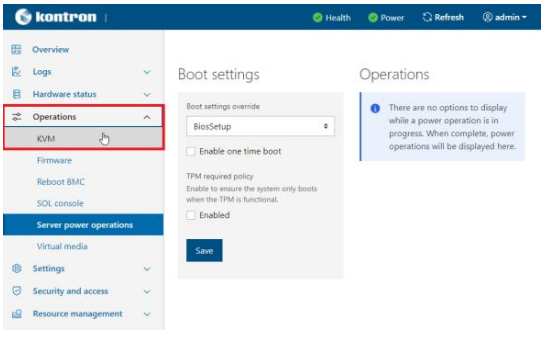
Launching the KVM

Step_1	From the left-side menu of the BMC Web UI, click on **Operations** and then on **KVM** .	
Step_2	A new browser window opens and displays the virtual server screen.	

Mounting the operating system image via virtual media

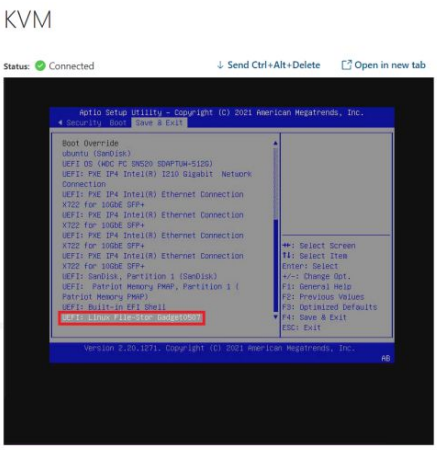
Step_1	From the **Operations** menu, select **Virtual media** .	
Step_2	Click on **Add file** to browse for the ISO file.	
Step_3	Click on **Start** to access virtual media from the OS.	

Accessing the UEFI/BIOS setup menu

Step_1	From the BMC Web UI, click on the **Power** button.	
Step_2	From the **Reboot server** section, select **Orderly** and then click on **Reboot** .	
Step_3	From the **Operations** menu, click on **KVM**.	
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...".	

		
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.	

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.	

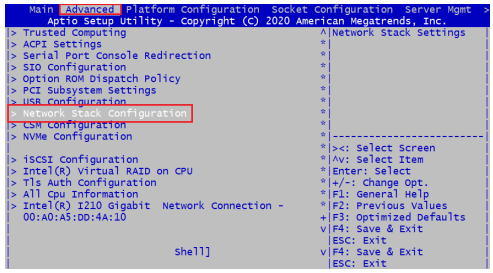
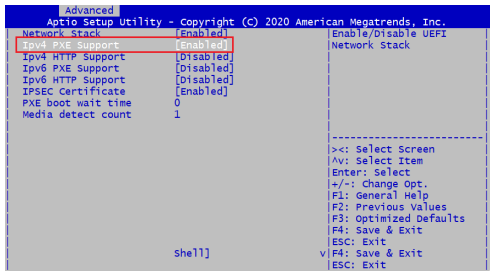
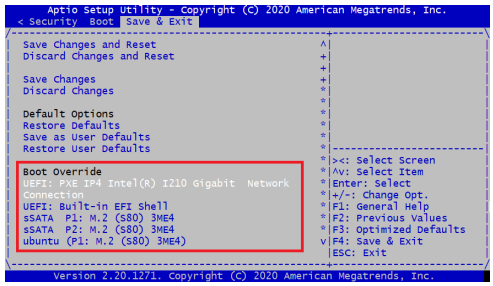
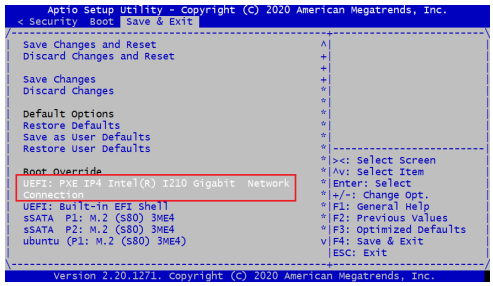
Completing operating system installation

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)

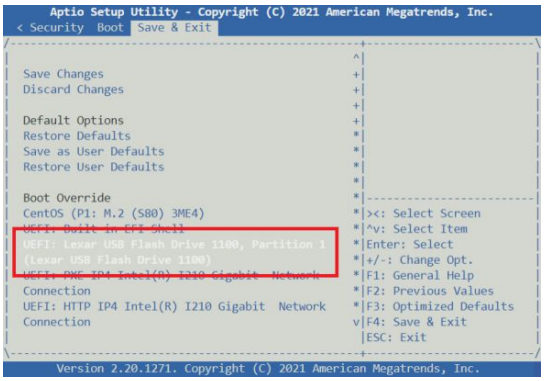
Relevant sections:
Accessing the UEFI or BIOS
Platform power management

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.	
Step_2	Set **Network Stack** to **Enabled** . Set **IPv4 PXE Support** or **IPv6 PXE Support** , depending on the application, to **Enabled** .	
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.	
Step_5	Choose the PXE option desired.	

Installing an OS on a server using a USB storage device

Relevant sections:
Accessing the UEFI or BIOS
Platform power management

Step_1	Create a bootable USB key using the appropriate software. **NOTE:** RUFUS is recommended.	
Step_2	Insert the USB key into 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 **Save & Exit** menu and then to the **Boot Override** section.	
Step_5	Choose the USB option desired.	

Verifying operating system installation

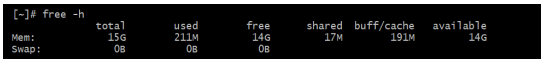
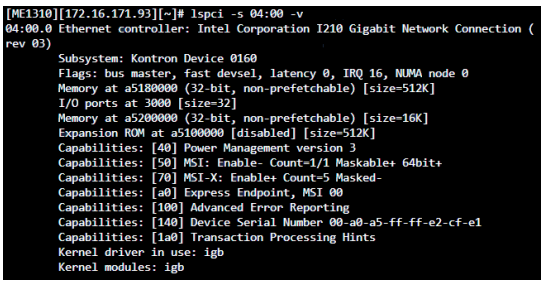
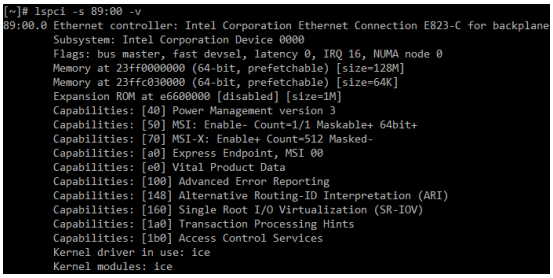
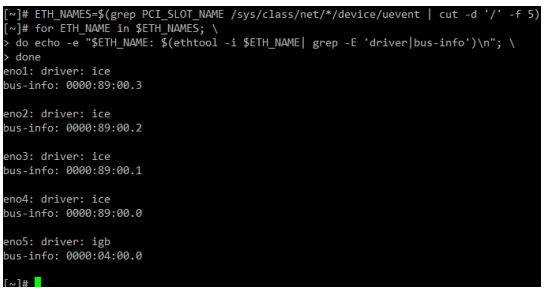
Table of contents

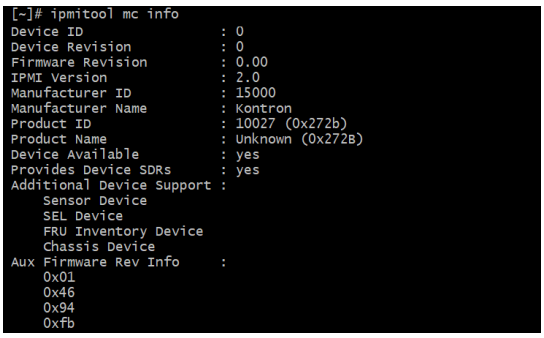
Relevant sections:

- Product architecture
- PCI mapping
- Accessing the operating system of a server
- Common software installation

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** **NOTE:** Updating the packages may take a few minutes.	
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**	
Step_5	Verify that all the storage devices are detected. LocalServer_OSPrompt:~# **lsblk**	
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.	
Step_7	Confirm the data plane network interface controllers are loaded by the **ice** driver. LocalServer_OSPrompt:~# **lspci -s 89:00 -v** **NOTE:** You should discover up to four 25GbE NIC.	
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 25GbE NIC.	

	NOTE: You should discover one 1GbE NIC and up to four 25GbE 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 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**	
Step_11	Verify communication between the operating system and the BMC. LocalServer_OSPrompt:~# **ipmitool mc info**	

Operating system power management states

The ME1310 platform does not support power management states. Please refer to Disabling sleep states in Linux for more information.

Platform resources for customer application

Table of contents

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.
3	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

Code example

The code example provided is in C.
Value 0x01 must be written to the I/O register 0xA0F (byte wide).

```
#include <sys/io.h>
int main(void)
{
iopl(3);
outb(0x01, 0xa0f);
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.

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

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 PCIe 2 mbox=50" > $sensor_daemon_pipe
  sleep 2
  echo "Temp PCIe 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
Configuring sensors and thermal parameters

Listing the available FRUs

Step_1	To verify if a specific PCIe add-in card can be registered in the virtual FRU, use the following command. RemoteComputer_OSPrompt:~# **cur l -k -s --request GET --url [ROOT_URL] /redfish/v1/Managers/bmc | jq .Oem.Kontron.VirtualPcieFru**

```
curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/M
anagers/bmc | jq .Oem.Kontron.VirtualPcieFru
{
  "AvailableFrus": [
    "P3iMB"
  ],
  "PCIe1": "P3iMB",
  "PCIe2": ""
}
```

Adding a virtual FRU

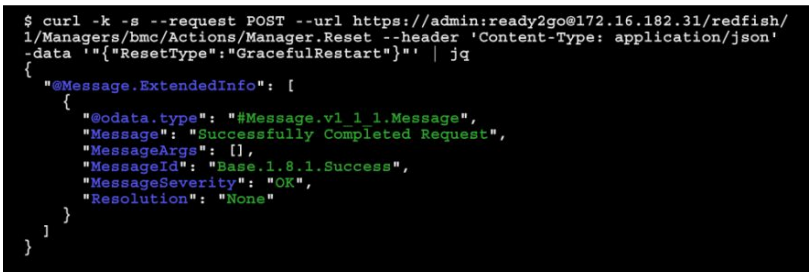
Step_1	Add a PCIe card to the virtual FRU using the following command. PCIE_SLOT can either be PCIe1 or PCIe2. RemoteComputer_OSPrompt:~# **curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc --header "'Content-Type: application/json'" --data '{"Oem": {"Kontron": {"VirtualPcieFru": {"[PCIE_SLOT]": " [FRU] "} } } } ' | jq**

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/
v1/Managers/bmc --header "'Content-Type: application/json'" --data '{"Oem": {"Ko
ntron": {"VirtualPcieFru": {"PCIe1": "P3iMB"}}}}' | jq
{
  "Oem": {
    "Kontron": {
      "VirtualPcieFru": {
        "PCIe1": "P3iMB"
      }
    }
  }
}
```

Step_2	Reboot the BMC to apply the changes. RemoteComputer_OSPrompt:~$ **curl -k -s --request POST --url [ROOT_URL] /redfish/v1/ Managers /bmc/Actions/Manager.Reset --header "Content-Type: application/json" --data '{"ResetType":"GracefulRestart"}' | jq**

```
$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/
1/Managers/bmc/Actions/Manager.Reset --header 'Content-Type: application/json'
-data '"{"ResetType":"GracefulRestart"}"' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "Successfully Completed Request",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Success",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

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 -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc --header "'Content-Type: application/json'" --data '{"Oem": {"Kontron": {"VirtualPcieFru": {"[PCIE_SLOT]": ""} } } } ' | jq
	
Step_2	Reboot the BMC to apply the changes. RemoteComputer_OSPrompt:~$ curl -k -s --request POST --url [ROOT_URL] /redfish/v1/ Managers /bmc/Actions/Manager.Reset --header "Content-Type: application/json" --data '{"ResetType":"GracefulRestart"}' | jq
	

Platform installation for high availability

Table of contents

Common software installation

Table of contents

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

Required software tools

Tool	Description
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

Configuring and managing users

Configuring and managing BMC users

Table of contents

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.

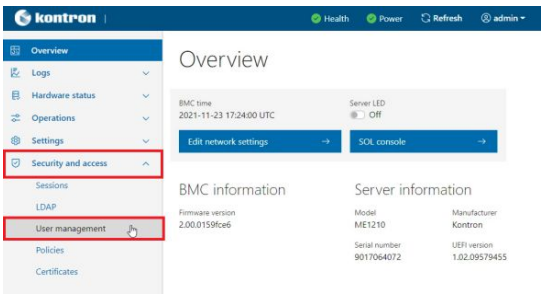
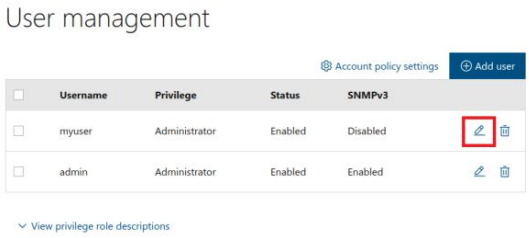
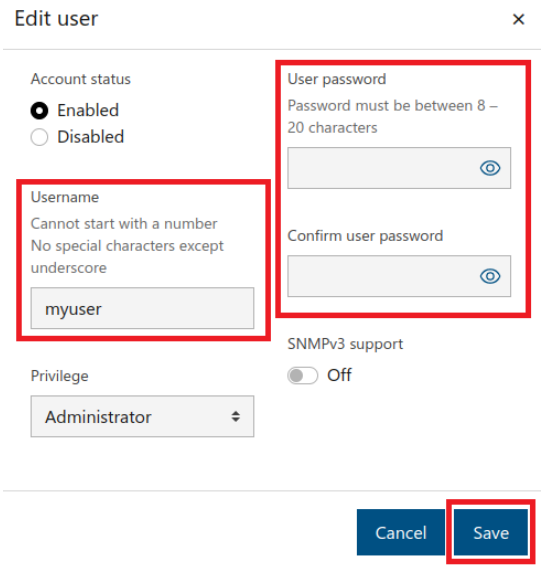
Roles		Description
BMC Web UI and Redfish	IPMI	
Admin	0x4 - Administrator	Users are allowed to configure everything regarding the BMC (including user management and network configuration). Users will have full administrative access.
Operator	0x3 - Operator	Users are allowed to view and control basic 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** .	
Step_2	Select the user to manage from the **User management** section.	
Step_3	Change the username and/or the password and confirm modifications by clicking on the **Save** button. **NOTE:** The password needs to be updated to update any other parameter.	

Using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

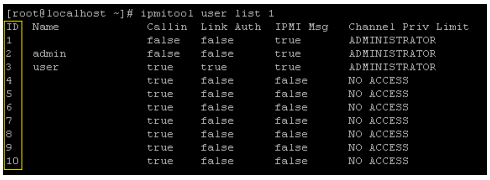
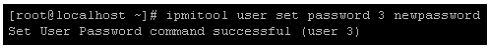
Step_1	List the users available. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/AccountService/Accounts | jq**

	$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/AccountService/Accounts | jq
	{
	"@odata.id": "/redfish/v1/AccountService/Accounts",
	"@odata.type": "#ManagerAccountCollection.ManagerAccountCollection",
	"Description": "BMC User Accounts",
	"Members": [
	{
	"@odata.id": "/redfish/v1/AccountService/Accounts/myuser"
	},
	{
	"@odata.id": "/redfish/v1/AccountService/Accounts/admin"
	}
	],
	"Members@odata.count": 3,
	"Name": "Accounts Collection"
	}

Step_2	Change the password. RemoteComputer_OSPrompt:~# **curl -k -s --request PATCH --url [ROOT_URL] /redfish/v1/ AccountService/Accounts/ [USERNAME] --header 'Content-type: application/json' --data '"{"Password":" [NEW_ PASSWORD] ", "UserName":" [NEW_USERNAME] "}"' | jq**
	$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/AccountService/Accounts/myuser --header 'Content-Type: application/json' --data '"{"Password": "Password7890!","UserName": "myuser2"}"' | jq

Using IPMI

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

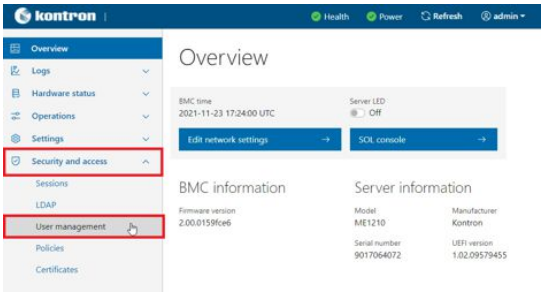
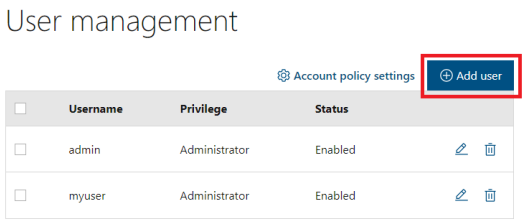
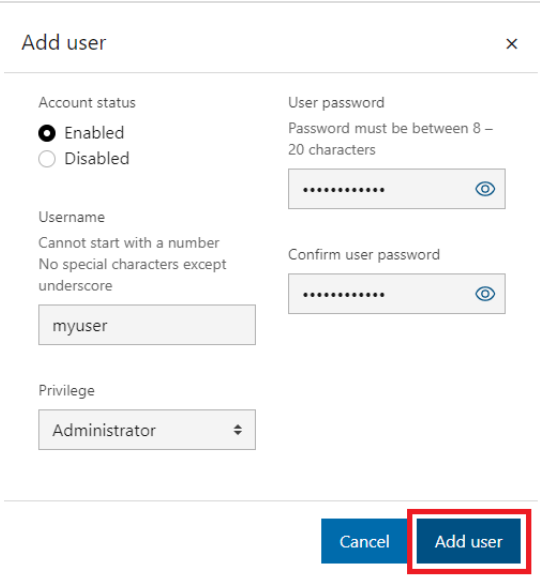
Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, print the BMC user list. LocalServer_OSPrompt:~# **ipmitool user list [LAN_CHANNEL]**	
Step_2	Identify the ID number of the user to be changed.	
Step_3	Change the user name. LocalServer_OSPrompt: ~# **ipmitool user set name [IPMI user ID] [new IPMI user name]** **NOTE:** The first and second user names of the user list are reserved fields and therefore can't be modified.	
Step_4	Verify that the user name has updated correctly by printing the user list. LocalServer_OSPrompt:~# **ipmitool user list [LAN_CHANNEL]**	
Step_5	Change the password. LocalServer_OSPrompt: ~# **ipmitool user set password [IPMI user ID] [new IPMI password]**	
Step_6	Verify that the credentials updated correctly by using an access method that requires a login. **NOTE:** Other parameters could limit the accessibility of the user that is trying to manage the BMC. Refer to ipmitool documentation.	

Adding a 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.**

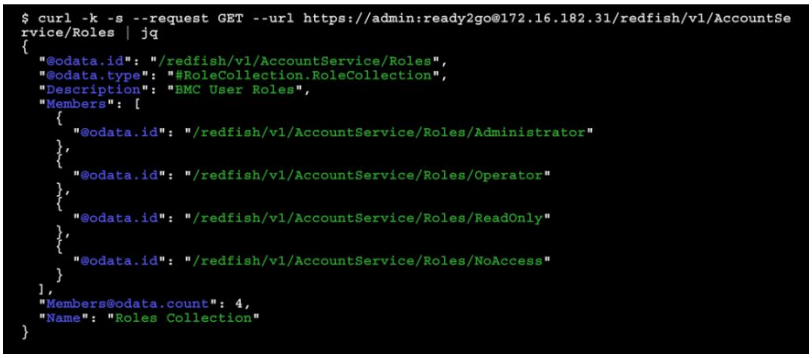
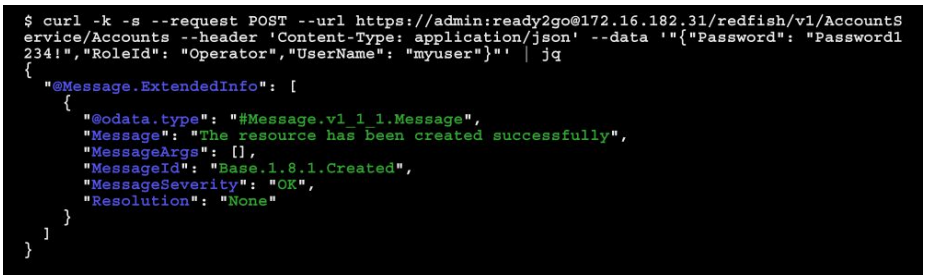
Using the Web UI

Refer to 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** .	
Step_2	Click on **Add user** .	
Step_3	Fill the required fields and click on **Add user** .	

Using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	List the privilege levels available. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/AccountService/Roles | jq**
	
Step_2	Using another user with administrator privilege, create the user. RemoteComputer_OSPrompt:~# **curl -k -s --request POST --url [ROOT_URL]/redfish/v1/AccountService/Accounts --header 'Content-Type: application/json' --data '"{"Password":" [PASSWORD] ","RoleId":" [ROLE_ID] ","UserName":" [USER_NAME] "}"' | jq**
	
Step_3	Verify that the user was created correctly by connecting to Redfish using its credentials.

Using IPMI

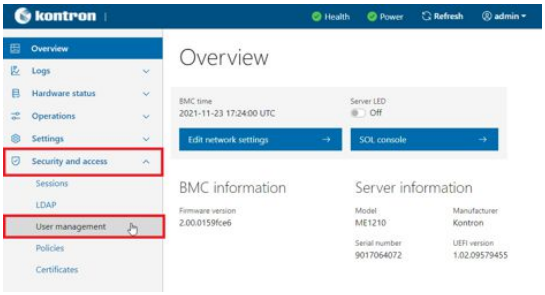
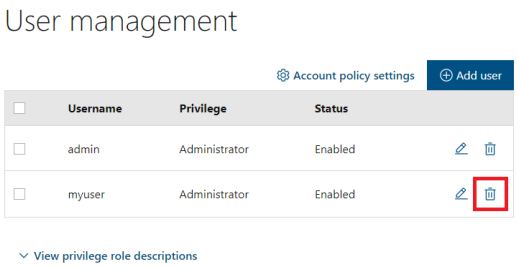
The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17** .

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]**	
Step_2	Create a user name. LocalServer_OSPrompt:~# **ipmitool user set name [IPMI user ID] [new IPMI user name]** **NOTE:** The first and second user names of the user list are reserved fields and therefore can't be modified.	
Step_3	Create the password. LocalServer_OSPrompt:~# **ipmitool user set password [IPMI user ID] [new IPMI password]**	
Step_4	Enable channel access and configure privilege level. LocalServer_OSPrompt:~# **ipmitool channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]**	
Step_5	Enable the user. LocalServer_OSPrompt:~# **ipmitool user enable [USER_ID]**	

Deleting a user

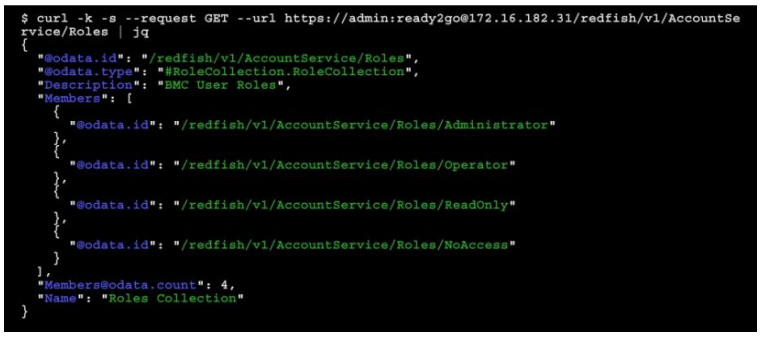
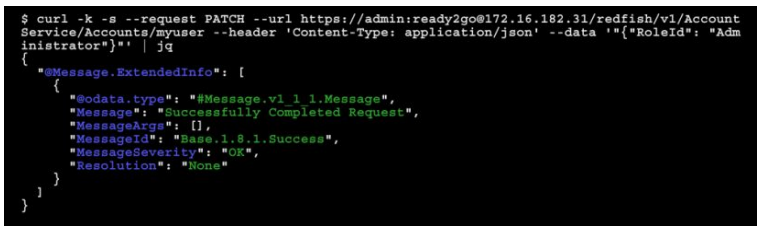
Using the Web UI

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** .	
Step_2	Select the user to delete from the **User management** section.	

Using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	List the privilege levels available. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/AccountService/Roles | jq**
	
Step_2	Change the privilege level. RemoteComputer_OSPrompt:~# **curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/AccountService/Accounts/ [USER_ID] --header 'Content-type: application/json' - -data '"{"RoleId":" [ROLE] "}"' | jq**
	

Using IPMI

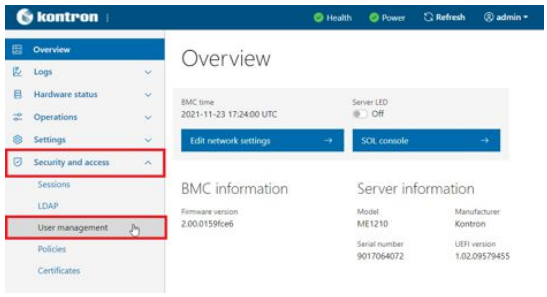
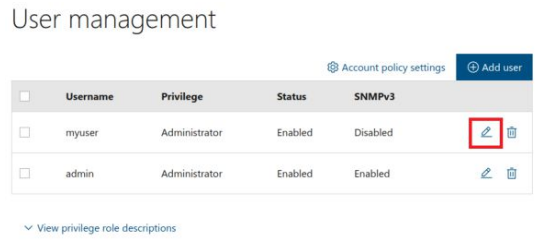
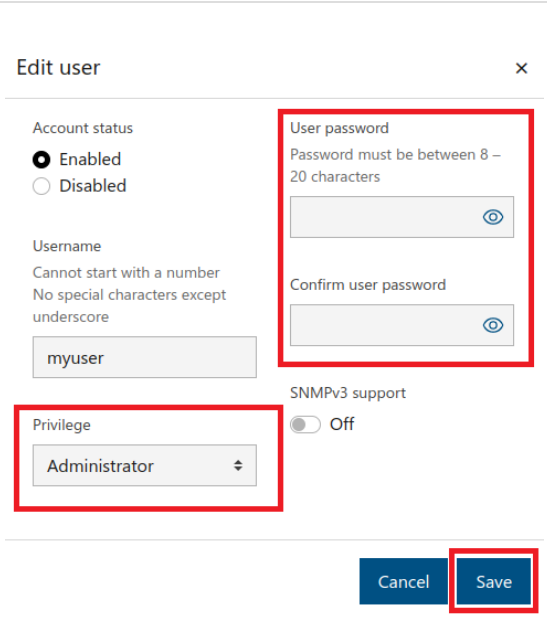
The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17** .
Users can't be deleted 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]**	
Step_2	Disable the user selected. LocalServer_OSPrompt:~# **ipmitool user disable [USER_ID]** **NOTE:** The first and second user names of the user list are reserved fields and therefore can't be disabled.	

Configuring privilege level

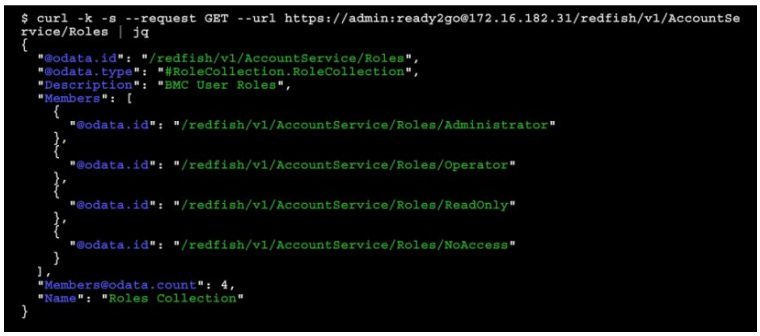
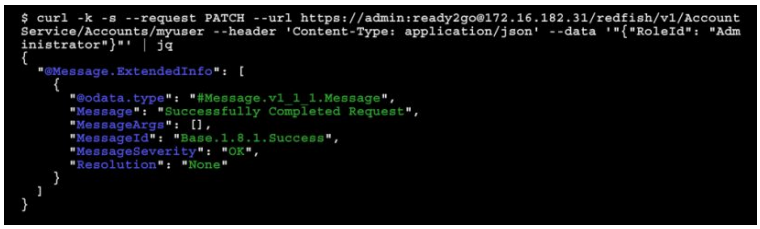
Using the Web UI

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** .	
Step_2	Select the user to manage from the **User management** section.	
Step_3	Change the privilege level in the **Privilege** field as well as the password and confirm the configuration by clicking on the **Save** button.	

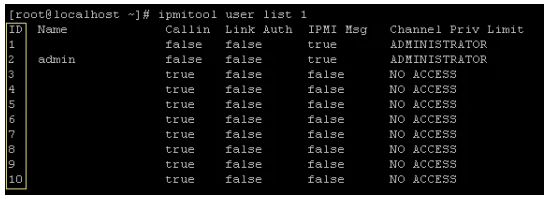
Using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	List the privilege levels available. RemoteComputer_OSPrompt:~# curl -k -s --request GET --url [ROOT_URL]/redfish/v1/AccountService/Roles | jq
	
Step_2	Change the privilege level. RemoteComputer_OSPrompt:~# curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/AccountService/Accounts/ [USER_ID] --header 'Content-type: application/json' - -data '"{"RoleId":" [ROLE] "}"' | jq
	

Using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -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]	
Step_2	List the privilege levels available. LocalServer_OSPrompt:~# ipmitool channel help	
Step_3	Set the privilege level for each channel. LocalServer_OSPrompt:~# ipmitool channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL] NOTE: The first and second user names of the user list are reserved fields and therefore can't be modified.	

Configuring and managing switch NOS users

Table of contents

Changes to the switch NOS configuration are not persistent after rebooting the switch NOS.
To preserve configurations, the current configuration needs to be saved to startup-config.
From the switch NOS Web UI:

- Select **Maintenance** , **Configuration** and then **Save startup-config** . Click on **Save Configuration** to confirm the change.

From the switch NOS CLI:

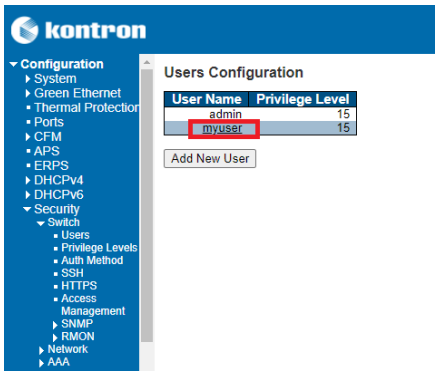
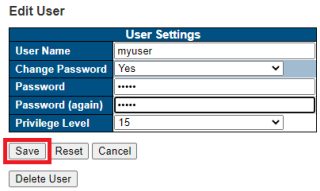
- LocalSwitchNOS_OSPrompt:~(config-if)# **end**
- LocalSwitchNOS_OSPrompt:~# **copy running-config startup-config**

Configuring switch NOS users using the switch NOS Web UI

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

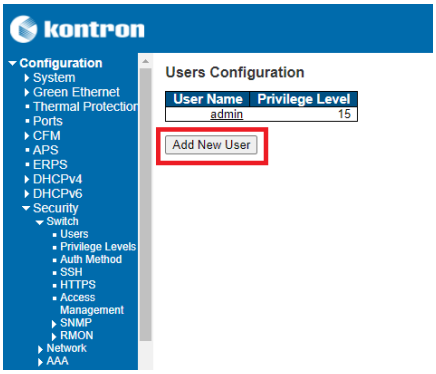
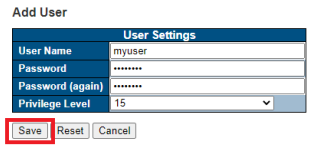
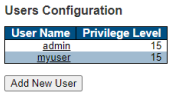
Changing the password of a user

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

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **Users** .	
Step_2	Click on the desired user.	
Step_3	Change the value of the **Change Password** dropdown menu to **Yes** .	
Step_4	Enter the password in fields **Password** and **Password (again)** .	
Step_5	Click on **Save** to confirm.	
Step_6	(Optional) To make the change persistent, save running-config to startup-config.	

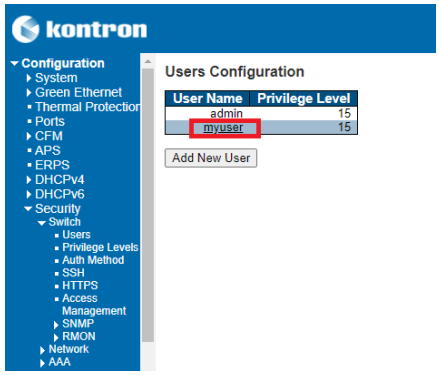
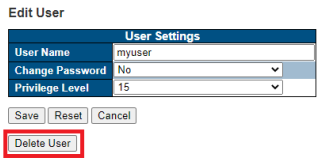
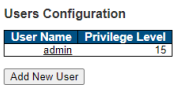
Adding a user

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

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **Users** .	
Step_2	Click on the **Add New User** button.	
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 NOS Web UI page.	
Step_4	Click on the **Save** button to add the user.	
Step_5	A new user should be displayed in the user list.	
Step_6	(Optional) To make the change persistent, save running-config to startup-config.	

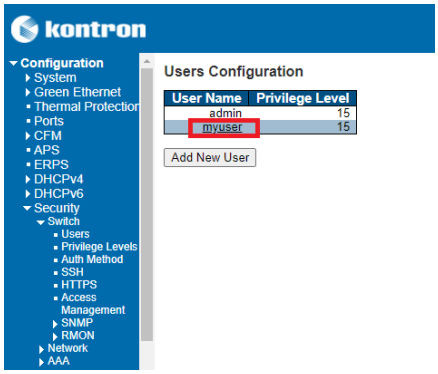
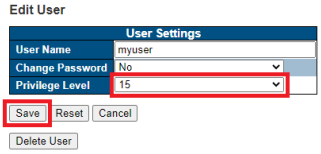
Deleting a user

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

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **Users** .	
Step_2	Click on the desired user.	
Step_3	Click on the **Delete User** button.	
Step_4	The user should be removed from the user list.	
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring privilege level

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

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **Users** .	
Step_2	Click on the desired 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 NOS Web UI page.	
Step_4	Click on the **Save** button to confirm.	
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring switch NOS users using the switch NOS CLI

Changing the password of a user

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 CLI .

Step_1	Access the configuration setup menu. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`
Step_2	Change the password. LocalSwitchNOS_OSPrompt:~(config)# **username [USERNAME] privilege [PRIVILEGE_LEVEL] password unencrypted [NEW_PASSWORD]**	`(config)# username user privilege 15 password unencrypted newPassword`
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Adding a user

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 CLI .

Step_1	Access the configuration setup menu. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`
Step_2	Add the user by entering its username, privilege level and password. LocalSwitchNOS_OSPrompt:~(config)# **username [USERNAME] privilege [PRIVILEGE_LEVEL] password unencrypted [PASSWORD]**	`(config)# username user privilege 15 password unencrypted Password`
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Deleting a user

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 CLI .

Step_1	Access the configuration setup menu. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`
Step_2	Delete the user. LocalSwitchNOS_OSPrompt:~(config)# **no username [USERNAME]**	`(config)# no username myuser` `(config)#`
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring privilege level

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 CLI .

Step_1	Access the configuration setup menu. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`
Step_2	To change the privilege level of a user, reconfigure the user and change its privilege level. LocalSwitchNOS_OSPrompt:~(config)# **username [USERNAME] privilege [NEW_PRIVILEGE_LEVEL] password unencrypted [PASSWORD]**	`(config)# username user privilege 11 password unencrypted Password`
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring date and time

Configuring BMC date and time

Table of contents

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

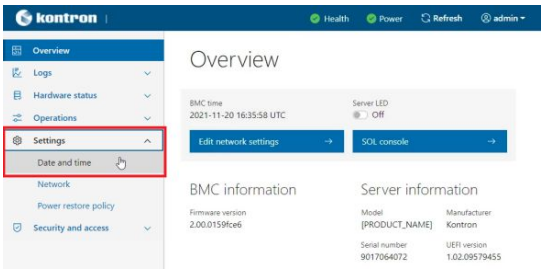
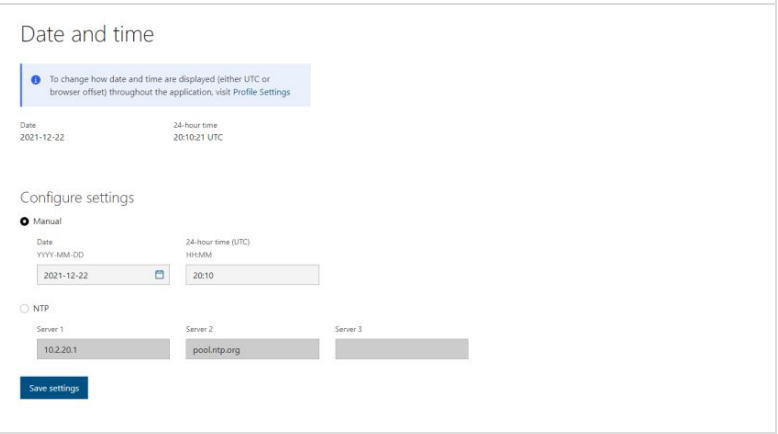
The BMC date and time can be set using:

- The BMC Web UI
- Redfish
- IPMI

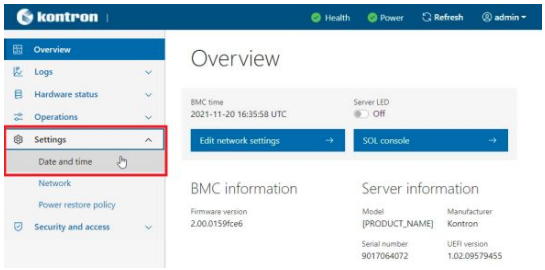
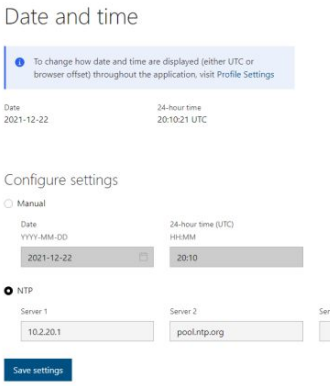
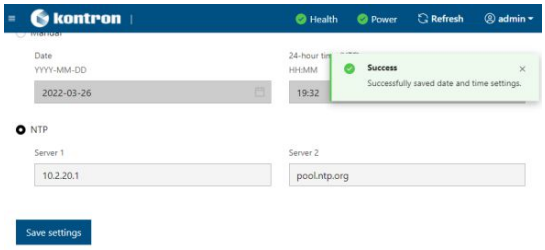
Configuring the BMC date and time using the Web UI

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

Manually c onfiguring the BMC date and time using the Web UI

Step_1	From the left-side menu, select **Settings** and then **Date and time** .	
Step_2	Select **Manual** and configure the date and time.	
Step_3	Click on the **Save settings** button.	

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** .	
Step_2	Select **NTP**.	
Step_3	Enter one or multiple NTP server addresses.	
Step_4	Click on the **Save settings** button.	
Step_5	A success message should appear upon successful configuration.	

Configuring the BMC date and time using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Manually c onfiguring the BMC date and time using Redfish

Step_1	If NTP is enabled, disable it. RemoteComputer_OSPrompt:~$ curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/ Managers/bmc /NetworkProtocol --header 'Content-Type: application/json' --data '"{"NTP": {"ProtocolEnabled": false}}"' | jq
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '"{"NTP": {"ProtocolEnabled": false}}"' | jq`
Step_2	Set the date and time manually using the following command. RemoteComputer_OSPrompt:~$ curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/ Managers/bmc --header 'Content-Type: application/json' - -data '"{"DateTime": "[DATE_TIME]"}"' | jq

	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header 'Content-Type: application/json' --data '"{"DateTime": "2021-12-21T18:36:59+00:00"}"' | jq`
	`{`
	`"DateTime": "2021-12-21T18:36:59+00:00"`
	`}`

Step_3	Verify BMC current date and time. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/ Managers/bmc | jq .DateTime

	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc | jq .DateTime`
	`{`
	`"DateTime": "2021-12-21T18:39:59+00:00",`
	`}`

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 -s --request PATCH --url [ROOT_URL]/redfish/v1/ Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '"{"NTP": {"NTPServers": [[NTP_SERVERS]],"ProtocolEnabled": true}}"' | jq `$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '"{"NTP": {"NTPServers": ["pool.ntp.org","10.2.20.1"],"ProtocolEnabled": true}}"' | jq`

Step_2	Verify BMC current date and time.
	RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/ Managers/bmc | jq .DateTime
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc | jq .DateTime`
	`{`
	`"DateTime": "2021-12-21T18:39:59+00:00",`
	`}`

Configuring the BMC date and time using IPMI

It is only possible to set time manually using IPMI.

Manually configuring the B MC date and time using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -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 System Event entries will be present in the SEL list.	`ipmitool sel list`
	`1 | 11/14/2018 | 17:07:10 | Event Logging Disabled #0x07 | Log area reset/cleared | Asserted`
	`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 | 17:06:58 | 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** https://github.com/ipmitool/ipmitool.git
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

It is not possible to manually set the date and time in the switch NOS. NTP or PTP must be used as a time source.
I f no NTP or PTP source is available on the network, the customer's OS on the integrated server can act as an NTP server . Please refer to your OS documentation.

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

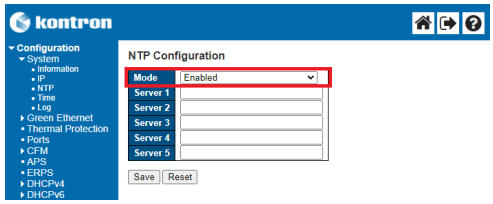
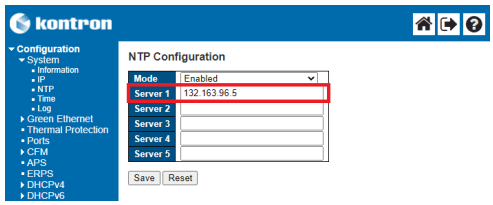
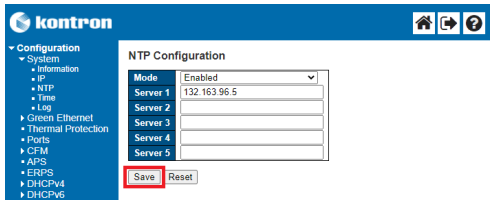
From the switch NOS CLI:
- LocalSwitchNOS_OSPrompt:~(config-if)# **end**
- LocalSwitchNOS_OSPrompt:~# **copy running-config startup-config**

Configuring the switch NOS date and time source based on the NTP

The switch NOS date and time source can be configured using:
- The switch NOS Web UI
- The switch NOS CLI

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

Access the switch NOS 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 Saving the current configuration using the Web UI .

Step_1	From the left-side menu, select **Configuration, System,** and then **NTP** .	
Step_2	Enable the NTP service by changing the value from the **Mode** dropdown menu to **Enabled** .	
Step_3	Enter the NTP server's address or hostname. **NOTE:** To enter a server hostname, a DNS service must be configured.	
Step_4	Repeat the previous step to add multiple NTP servers if needed.	
Step_5	Click on the **Save** button.	
Step_6	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the switch NOS date and time source based on the NTP using the CLI

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

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.
		`(config) # ntp server 1 ip-address 132.163.96.5`
		OR
		`(config)# ntp server 1 ip-address pool.ntp.org`

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**
		`# show ntp status`
		`NTP Mode : enabled`
		`Idx  Server IP host address (a.b.c.d) or a host name string`
		`---  ----------`
		`1  132.163.96.5`
		`2`
		`3`
		`4`
		`5`

Step_6	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the switch NOS date and time source based on the PTP

For information on using PTP as source for date and time, refer to Configuring synchronization .

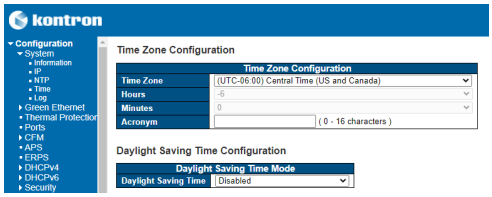
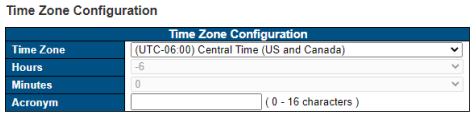
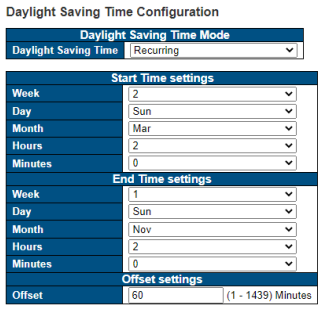
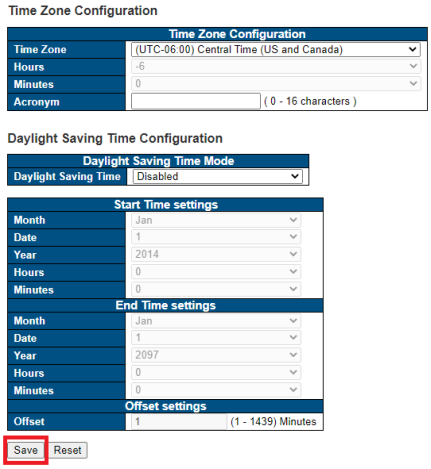
Configuring the switch NOS time zone and daylight saving time

The switch NOS time zone and daylight saving time can be configured using:

- The switch NOS Web UI
- The switch NOS CLI

Configuring the switch NOS time zone and daylight saving time using the Web UI

Access the switch NOS 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 Saving the current configuration using the Web UI .

Step_1	From the left-side menu, select **Configuration, System** and then **Time** .	
Step_2	Configure the time zone by selecting it from the **Time Zone** dropdown menu.	
Step_3	Configure the **Daylight Saving Time** .	
Step_4	Click on **Save** .	
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the switch NOS time zone and daylight saving time using the CLI

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

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**

	`(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: 0`
	`Daylight Saving Time Offset : 60 (minutes)`

Step_5	(Optional) To make the change persistent, save running-config to startup-config.

Configuring networking

Configuring the BMC networking

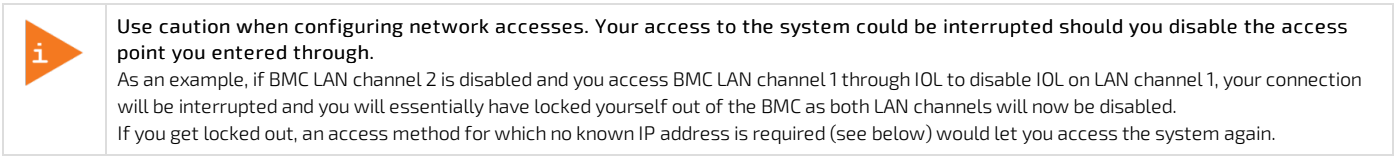
Table of contents

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.



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.
If you get locked out, an access method for which no known IP address is required (see below) would let you access the system again.

Relevant sections:

- Discovering platform IP addresses
- Product architecture

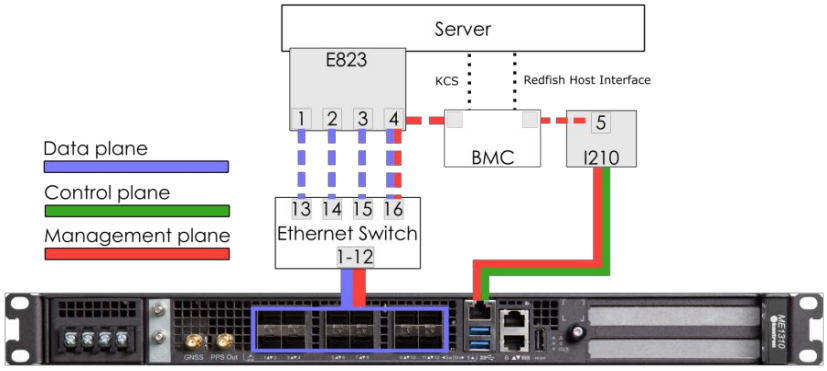
Selecting an access method for BMC networking configuration

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 Accessing the UEFI/BIOS using a serial console (physical connection) 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 (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 Accessing a BMC using Redfish 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 Accessing a BMC using IPMI over LAN (IOL) or Accessing a BMC using IPMI (KCS) for access in instructions.
  - Use the UEFI/ BIOS setup menu. Refer to Accessing the UEFI or BIOS for access instructions.

BMC network architecture

Ethernet switch IO module option



In a 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 → switch port 16 *

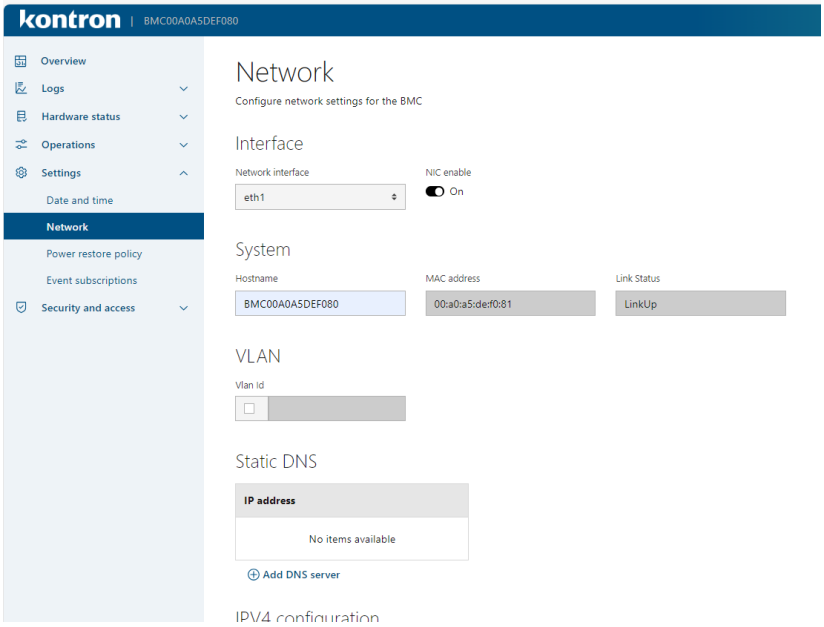
* The BMC can then communicate through SFP ports Sw 1 to 12, depending on switch configuration.

Pass-through IO module option

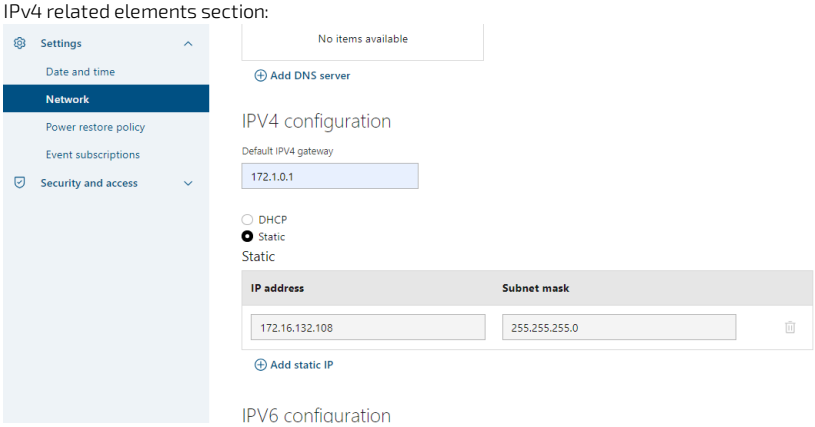
This option is planned for development. Please contact Kontron sales .

Network settings configurable thru WebUI

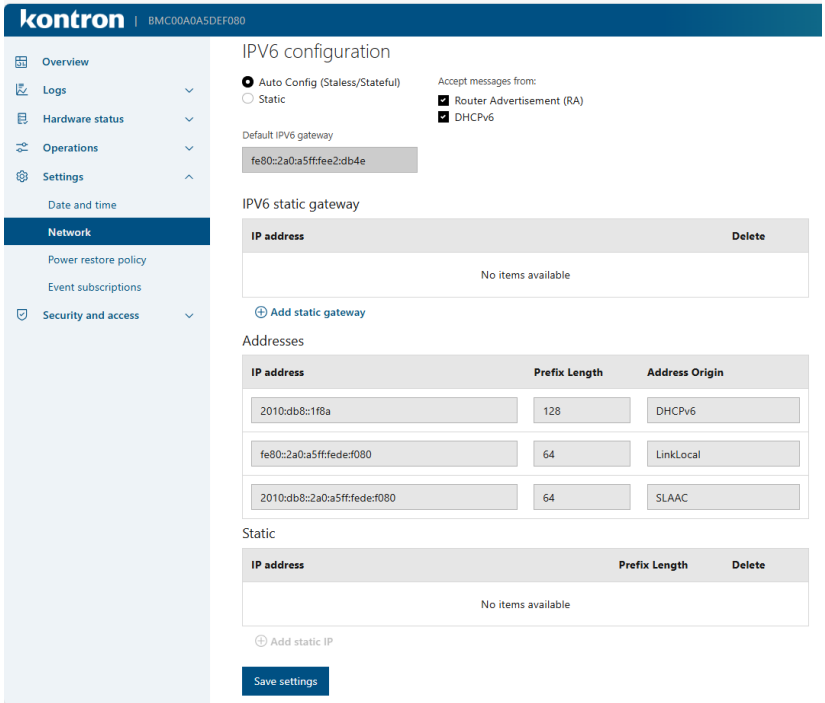
To access the Network Setting page, from the left-side menu of the BMC Web UI, select **Settings** and then **Network** .
The page contains 3 main sections :
General/Common elements section:



IPv4 related elements section:



IPv6 related elements section:



Element	Description
Common/General section	
Network Interface	Selection of the network interface to get/set its configuration
NIC Enable	Enable/Disable the selected Network Interface
Hostname	Shows BMC Host Name.
MAC Address	Shows interface MAC address
Link Status	Indicate if selected interface link is Up or Down
VLAN Id	Use to set/show ID on VLAN configuration
Static DNS table	Table to configure/list static DNS of the interface.
IPv4 section	
Default IPv4 Gateway	Shows the default IPv4 Gateway assigned to the interface (read only for DHCP mode, writable for Static mode).
DHCP/Static	IPv4 addresses assignation mode: • DHCP: Select this option to dynamically configure IPv4 address using Dynamic Host Configuration Protocol (DHCP). • Static: Select this option to manually create the interface IP addresses.
IPv4 addresses table	Table of IPv4 addresses and subnet mask of the selected interface. • If DHCP: The table is read only and lists address(es) got from a DHCP server. • If Static: User can change/delete/create new IPv4 addresses in this table.
IPv6 section	

Auto Config/Static	IPv6 addresses assignation mode:
	• Auto Config: Select this option for dynamic IPv6 address configuration using one (or both) of these 2 services:
	  ◦ DHCPv6
	  ◦ Router Advertisement (RA)
	• Static: Select this option to manually create the interface IPv6 addresses.
	In either of these modes, the BMC also automatically creates a “link local” address (starts with FE80) for the interface.

Default IPv6 Gateway	Shows the default IPv6 Gateway assigned to the interface (read only)
IPv6 Static Gateway table	Table used to configure/change/delete IPv6 Static gateways.
Addresses table	Table listing all IPv6 addresses, prefix length and origin of the selected interface. Origins can be Static, LinkLocal, DHCPv6 or SLAAC (Stateless Address Auto-Configuration). This table is read only.
Static table	Table used to configure/change/delete manually IPv6 adresses and their prefix length (when Static assignation mode selected).

Network settings configurable thru Redfish

This page lists the redfish properties relevant to features/settings our BMC currently support regarding network settings.
Snapshot of elements we get with curl command:
curl -k -s --request GET --url https://<user>:<pw>@<BmcIP>/redfish/v1/Managers/bmc/EthernetInterfaces/<interface> | jq

```
{
  "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth1",
  "@odata.type": "#EthernetInterface.v1_4_1.EthernetInterface",
  "DHCPv4": {
    "DHCPEnabled": true,
    "UseDNSServers": true,
    "UseDomainName": true,
    "UseNTPServers": true
  },
  "DHCPv6": {
    "OperatingMode": "Enabled",
    "UseDNSServers": true,
    "UseDomainName": true,
    "UseNTPServers": true
  },
  "Description": "Management Network Interface",
  "FQDN": "BMC00A0A5DEF080",
  "HostName": "BMC00A0A5DEF080",
  "IPv4Addresses": [
    {
      "Address": "172.16.132.109",
      "AddressOrigin": "DHCP",
      "Gateway": "172.16.0.1",
      "SubnetMask": "255.255.0.0"
    }
  ],
  "IPv4StaticAddresses": [],
  "IPv6AddressPolicyTable": [],
  "IPv6Addresses": [
    {
      "Address": "fe80::2a0:a5ff:fede:f081",
      "AddressOrigin": "LinkLocal",
      "AddressState": null,
      "PrefixLength": 64
    }
  ],
  "IPv6DefaultGateway": "0:0:0:0:0:0:0:0",
  "IPv6StaticAddresses": [],
  "IPv6StaticDefaultGateways": [],
  "Id": "eth1",
  "InterfaceEnabled": true,
  "LinkStatus": "LinkUp",
  "MACAddress": "00:a0:a5:de:f0:81",
  "Name": "Manager Ethernet Interface",
  "NameServers": [
    "10.232.30.5"
  ],
  "SpeedMbps": 0,
  "StatelessAddressAutoConfig": {
    "IPv6AutoConfigEnabled": false
  },
  "StaticNameServers": [],
  "Status": {
    "Health": "OK",
    "HealthRollup": "OK",
    "State": "Enabled"
  },
  "VLANs": {
    "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces/eth1/VLANs"
  }
}
```


Relevant properties list			
Property	**Type**	**Attribute**	**Description**
DHCPv4	object		DHCPv4 configuration for this interface.
->DHCPEnabled	bool	read/write	An indication of whether DHCP v4 is enabled on this Ethernet interface.
->UseDNSServers	bool	read/write	An indication of whether this interface uses DHCP v4-supplied DNS servers.
->UseDomainName	bool	read/write	An indication of whether this interface uses a DHCP v4-supplied domain name.
->UseNTPServers	bool	read/write	An indication of whether the interface uses DHCP v4-supplied NTP servers.
DHCPv6	object		DHCPv6 configuration for this interface.
->OperatingMode	string	read/write	Determines the DHCPv6 operating mode for this interface. *Find the possible property values in Redfish documentation****
->UseDNSServers	bool	read/write	An indication of whether the interface uses DHCP v6-supplied DNS servers.
->UseDomainName	bool	read/write	An indication of whether this interface uses a DHCP v6-supplied domain name.
->UseNTPServers	bool	read/write	An indication of whether the interface uses DHCP v6-supplied NTP servers.
IPv4Addresses	object(array)		The IPv4 addresses currently in use by this interface.
->Address	string	read/write	The IPv4 address
->AddressOrigin	string	read/write	This indicates how the address was determined. *Find the possible property values in Redfish documentation****
->Gateway	string	read/write	The IPv4 gateway for this address.
->SubnetMask	string	read/write	The IPv4 subnet mask
IPv4SaticAddresses	object(array)	read/write	The IPv4 addresses currently in use by this interface.

->Address	string	read/write	The IPv4 address
->Gateway	string	read/write	The IPv4 gateway for this address.
->SubnetMask	string	read/write	The IPv4 subnet mask
IPv6Addresses	object(array)		The IPv6 addresses currently in use by this interface.
->Address	string	read/write	A valid IPv6 address.
->AddressOrigin	string	read only	This indicates how the address was determined. *Find the possible property values in Redfish documentation****
->AddressState	string	read only	The current RFC4862-defined state of this address. *Find the possible property values in Redfish documentation****
->PrefixLength	integer	read/write	The prefix length, in bits, of this IPv6 address.
IPv6DefaultGateway	string	read only	The IPv6 default gateway address in use on this interface.
IPv6StaticAddresses	object(array)		The IPv6 static addresses assigned to this interface.
->Address	string	read/write	A valid IPv6 address.
->PrefixLength	integer	read/write	The prefix length, in bits, of this IPv6 address.
IPv6StaticDefaultGateways	object(array)		The IPv6 static default gateways for this interface.
->Address	string	read/write	A valid IPv6 address.
->PrefixLength	integer	read only	The IPv6 network prefix length, in bits, for this address. *NOTE: we do not support gateways prefix length other then 128 (full length), so this field has been set to read only in our BMC*
InterfaceEnabled	bool	read/write	An indication of whether this interface is enabled.
LinkStatus	string	read only	The link status of this interface, or port. *Find the possible property values in Redfish documentation****
MACAddress	string	read/write	The currently configured MAC address of the interface, or logical port.
NameServers	array	read only	The DNS servers in use on this interface.
SpeedMbps	integer	read/write	The current speed, in Mbit/s, of this interface.
StatelessAddressAutoConfig	object		Stateless address autoconfiguration (SLAAC) parameters for this interface.
->IPv6AutoConfigEnabled	bool	read/write	An indication of whether IPv6 stateless address autoconfiguration (SLAAC) is enabled for this interface.
StaticNameServers	array	read/write	The statically-defined set of DNS server IPv4 and IPv6 addresses.
Status	object		The status and health of the resource and its subordinate or dependent resources.
->Health	string	read only	The health state of this resource in the absence of its dependent resources. *Find the possible property values in Redfish documentation****
->HealthRollup	string	read only	The overall health state from the view of this resource. *Find the possible property values in Redfish documentation****
->State	string	read only	The known state of the resource, such as, enabled. *Find the possible property values in Redfish documentation****
VLANs	object		The link to a collection of VLANs. *For details see Redfish documentation****

*** To get more details on these properties (and/or sub elements not listed in this table of these properties), refer to Redfish documentation (www.dmtf.org)

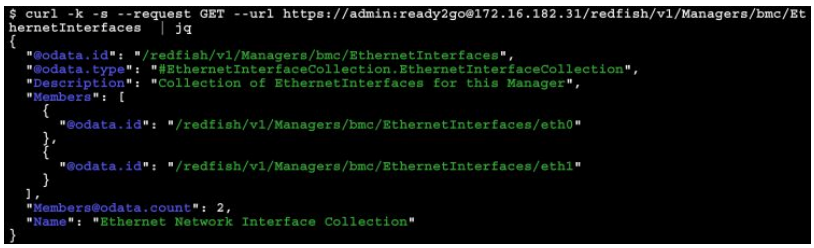
Enabling or disabling a BMC network interface

This can be achieved:

- Using Redfish
- Using the BMC Web UI
- Using IPMI

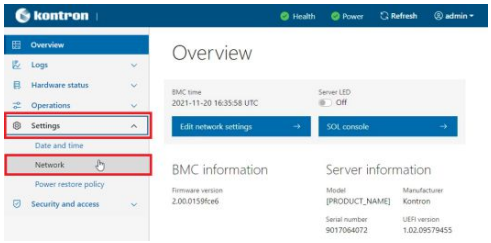
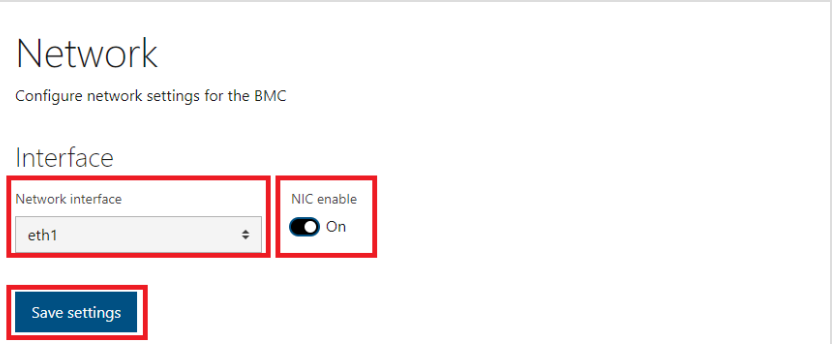
Enabling or disabling a BMC network interface using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish 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 -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/ | jq**
	
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 -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME] --header 'Content-Type: application/json' --data '{"InterfaceEnabled":[VALUE]}' | jq**
	

Enabling or disabling a BMC network interface 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** .	
Step_2	From the dropdown menu of the **Interface** section, select a network interface to configure.	
Step_3	Click on the **NIC enable** button to enable or disable the network interface.	
Step_4	Click on **Save settings** .	

Enabling or disabling a BMC network interface using IPMI

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

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.	

Configuring a static IP address

This can be achieved :

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

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

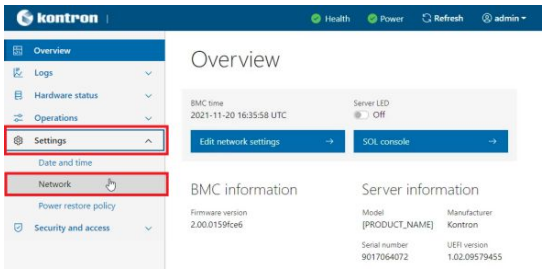
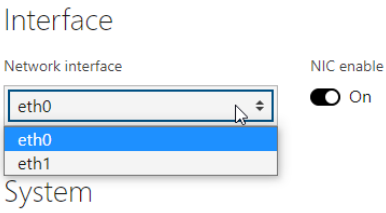
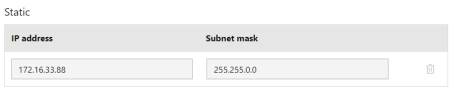
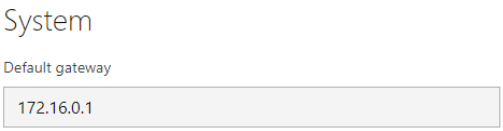
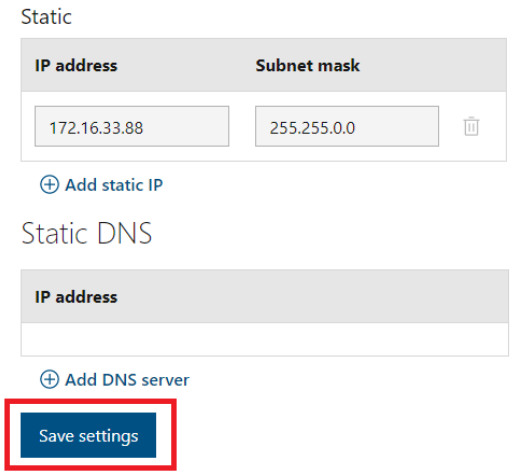
Configuring a static IP address using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish 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 -s --request PATCH --url** [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME] **--header 'Content-Type: application/json' --data '{"IPv4StaticAddresses": [{"Address": "[IP_ADDRESS]","SubnetMask": "[MASK]","Gateway": "[GATEWAY]"}]}' | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/EthernetInterfaces/eth1 --header 'Content-Type:application/json' --data '{"IPv4StaticAddresses": [{"Address": "172.16.182.32","SubnetMask": "255.255.0.0","Gateway": "172.16.0.1"}]}' | jq`

Configuring a static IP address using the BMC Web UI

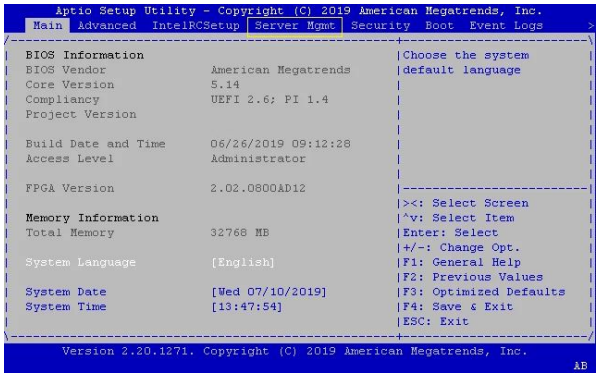
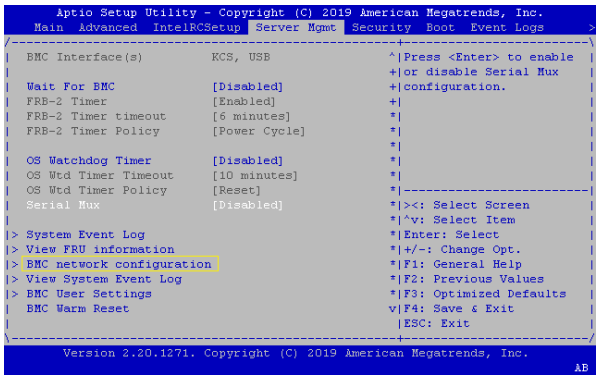
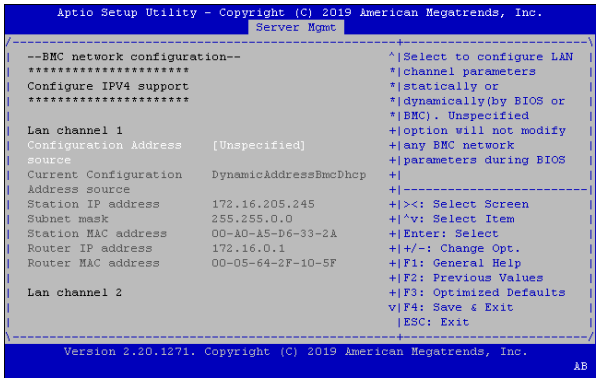
Refer to Accessing a BMC using the Web UI for access instructions.

Step_1	From the left-side menu of the BMC Web UI, select **Settings** and then **Network** .	
Step_2	Select the network interface to configure from the dropdown menu.	
Step_3	From the **IPV4** section, select **Static**.	
Step_4	From the **Static** section, configure the desired **IP address** and **Subnet mask** .	
Step_5	From the **System** section, configure the **Default gateway**.	
Step_6	Click on **Save settings**.	

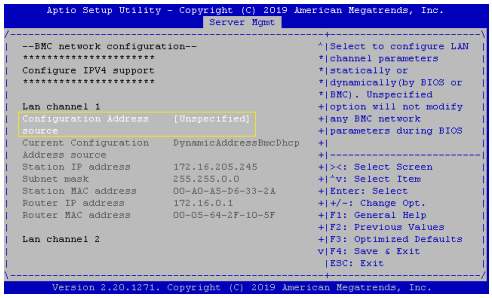
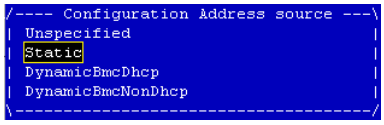
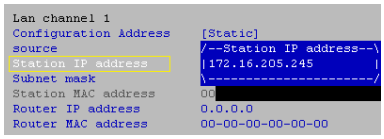
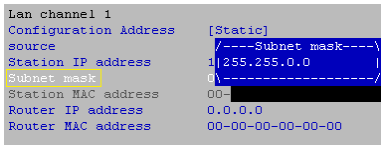
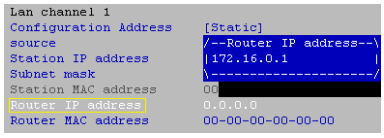
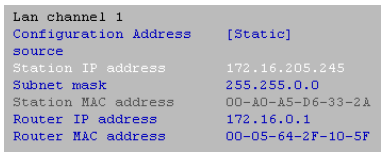
Configuring a static IP address using the UEFI/BIOS setup menu

Refer to Accessing the UEFI or BIOS for access instructions.

Accessing the BMC network configuration menu

Step_1	From the UEFI/BIOS menu, navigate to tab **Server Mgmt** .	
Step_2	Select **BMC network configuration** .	
Step_3	The **BMC network configuration** menu is displayed. **NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS .	

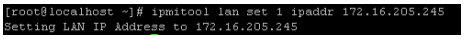
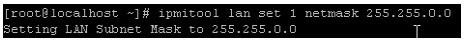
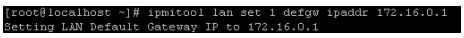
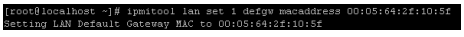
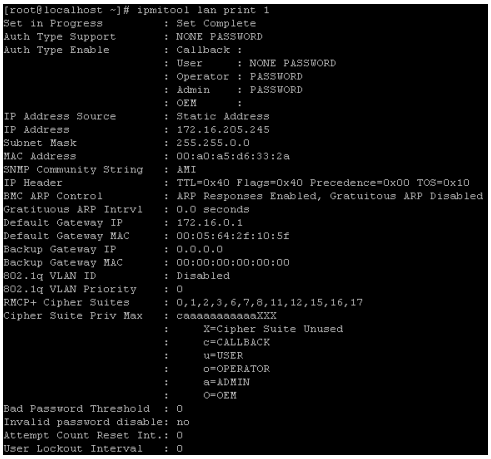
Configuring a static IP address using the UEFI/BIOS setup menu

Step_1	From the **BMC network configuration** menu, select the **Configuration Address source** option for the LAN interface to configure (LAN channel 1 in this example).	
Step_2	Select **Static** .	
Step_3	Change the **Station IP address** . **NOTE:** This is the BMC IP address (**BMC MNGMT_IP**).	
Step_4	Change the **Subnet mask** .	
Step_5	Change the **Router IP address** .	
Step_6	Confirm the configuration has changed and exit **BMC network configuration** using the **ESC** key.	

Configuring a static IP address using IPMI

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

Configuring a static IP address

Step_1	Set the IP source to static. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] ipsrc static**	
Step_2	Set the IP address to be used. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] ipaddr [NEW_IP]** **NOTE:** This is the BMC IP address (**BMC MNGMT_IP**). **NOTE:** It can take several seconds for an IP address to be set.	
Step_3	Set the subnet mask. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] netmask [NEW_MASK]** **NOTE:** It can take several seconds for a subnet mask to be set.	
Step_4	Set the default gateway IP address. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] defgw ipaddr [ROUTER_IP]** **NOTE:** It can take several seconds for a default gateway IP address to be set.	
Step_5	Set the default gateway MAC address. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] defgw macaddress [ROUTER_MAC]**	
Step_6	Verify that the configuration has changed. LocalServer_OSPrompt:~# **ipmitool lan print [LAN_CHANNEL]**	

Configuring a dynamic IP address using DHCP

This can be achieved:

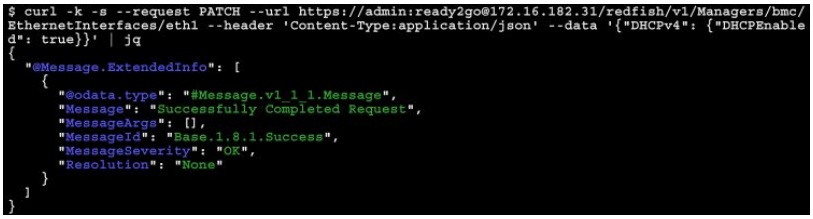
- Using Redfish
- Using the BMC Web UI
- Using the UEFI/BIOS setup menu
- Using IPMI

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

Configuring a dynamic IP address using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

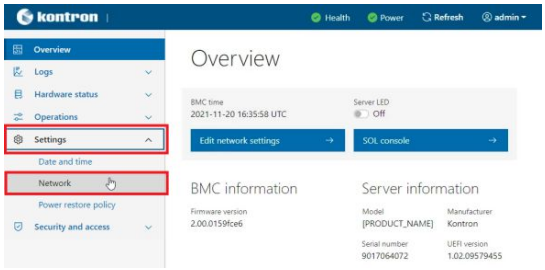
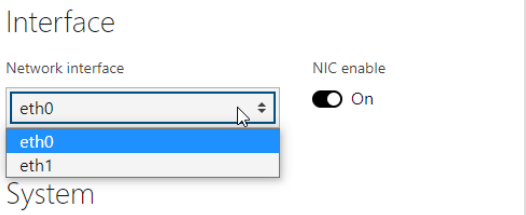
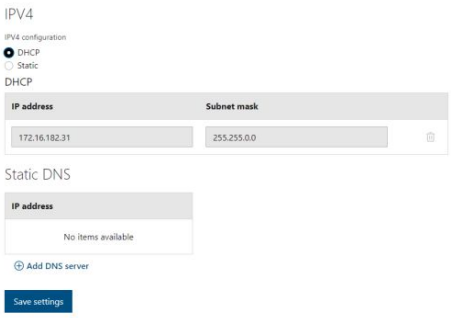
Step_1	To enable the DHCP addressing method in Redfish, PATCH the proper BMC network interface with the DHCP field. RemoteComputer_OSPrompt:~# **curl -k -s --request PATCH --url [ROOT_URL] /redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME] --header 'Content-Type: application/json' --data '{"DHCPv4": {"DHCPEnabled": true}}' | jq**



Configuring a dynamic IP address using the BMC Web UI

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

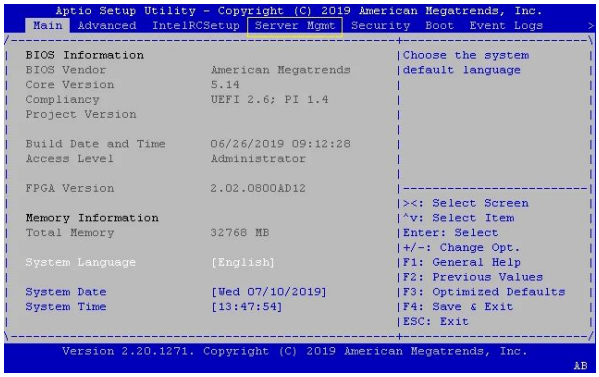
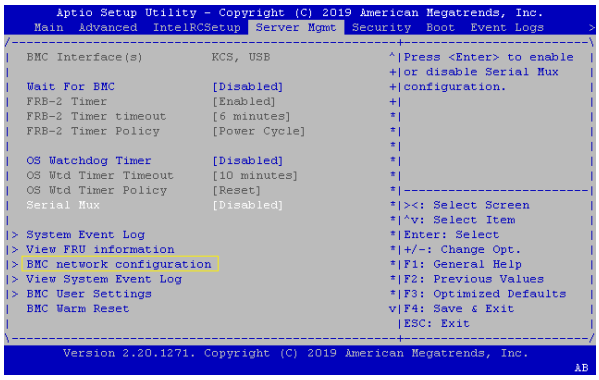
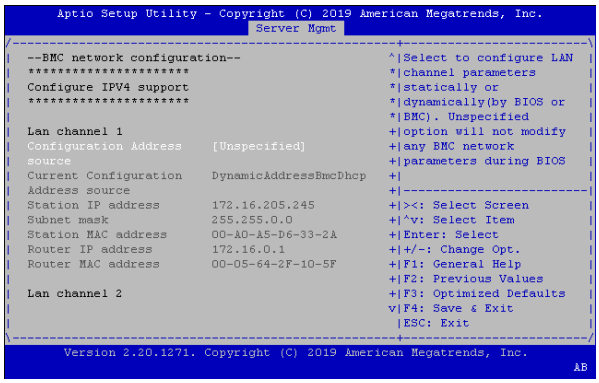
Configuring a dynamic IP address

Step_1	From the left-side menu of the BMC Web UI, select **Settings** and then **Network** .	
Step_2	Select the network interface to configure from the dropdown menu.	
Step_3	From the **IPV4** section, select **DHCP**.	
Step_4	Click on **Save settings**.	

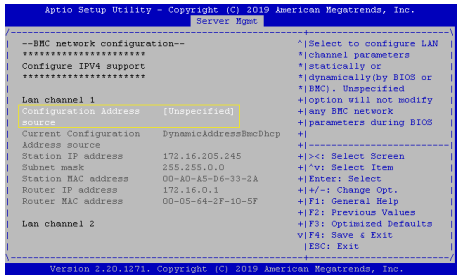
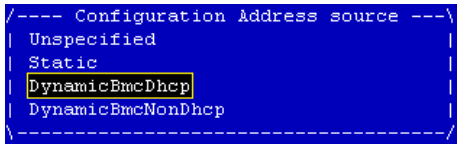
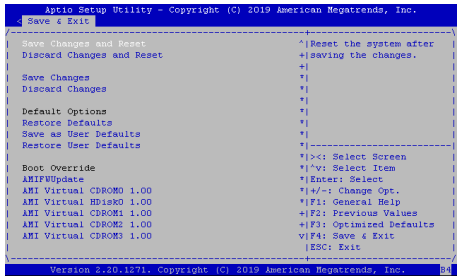
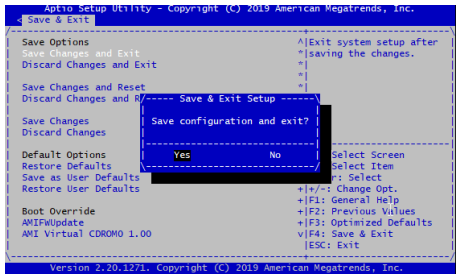
Configuring a dynamic IP address using the UEFI/BIOS setup menu

Refer to Accessing the UEFI or BIOS for access instructions.

Accessing the BMC network configuration menu

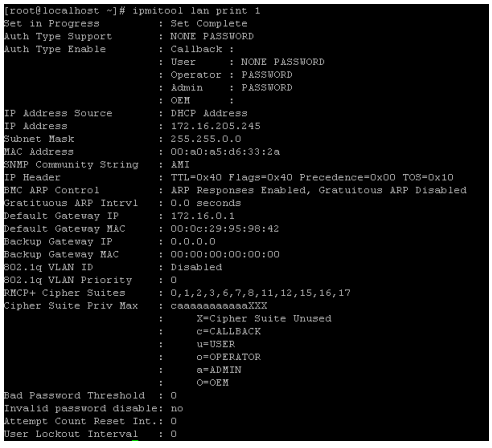
Step_1	From the UEFI/BIOS menu, navigate to tab **Server Mgmt** .	
Step_2	Select **BMC network configuration** .	
Step_3	The **BMC network configuration** menu is displayed. **NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS .	

Configuring a dynamic IP address using DHCP

Step_1	From the **BMC network configuration** menu, select the **Configuration Address source** option of the LAN interface to configure (LAN channel 1 in this example).	
Step_2	Select **DynamicBmcDhcp**.	
Step_3	Navigate to **Save & Exit**.	
Step_4	Select **Save Changes and Exit** . This will perform a server reset.	
Step_5	When the UEFI/ BIOS sign on screen is displayed, press the specified key to enter the UEFI/ BIOS setup menu. Then, access the **Server Mgmt** menu and select **BMC network configuration** . T he address displayed is your BMC IP address (BMC MNGMT_IP).	

Configuring a dynamic IP address using IPMI

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

Step_1	Set the IP source to DHCP. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] ipsrc dhcp** **NOTE:** Depending on the existing infrastructure, it may take several seconds to gather an IP from the DHCP server.	
Step_2	Verify that the configuration has changed. LocalServer_OSPrompt:~# **ipmitool lan print [LAN_CHANNEL]** **NOTE:** This is the BMC IP address (**BMC MNGMT_IP**).	

Configuring a VLAN for a BMC network interface

Given the ME1310 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 .

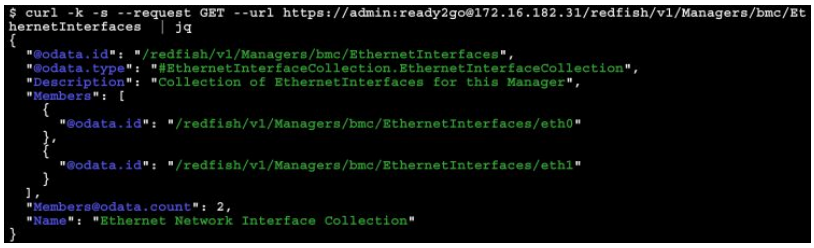
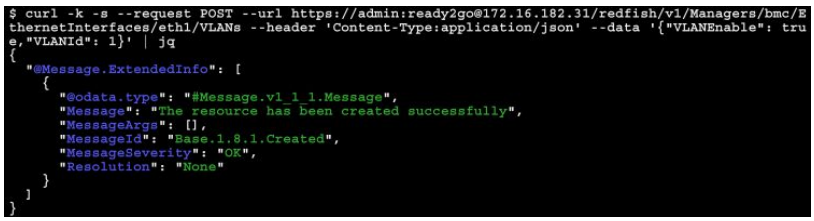
Assigning a VLAN

This can be achieved:

- Using Redfish
- Using the BMC Web UI
- Using IPMI

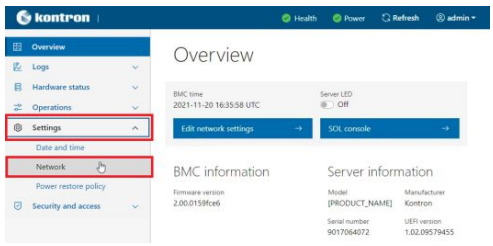
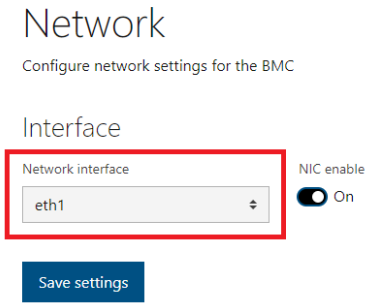
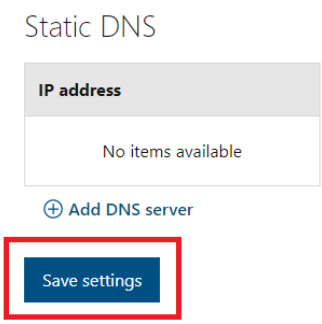
Assigning a VLAN u sing Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Select a BMC network interface and take note of its URL. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces | jq**
	
Step_2	Add a VLAN for the selected BMC network interface using the following command. RemoteComputer_OSPrompt:~# **curl -k -s --request POST --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]/VLANs --header 'Content-Type: application/json' --data '{"VLANEnable": true,"VLANId": [VLAN_ID] }' | jq**
	
Step_3	Configure an IP address for the VLAN interface created using one of the Redfish methods described in this section.

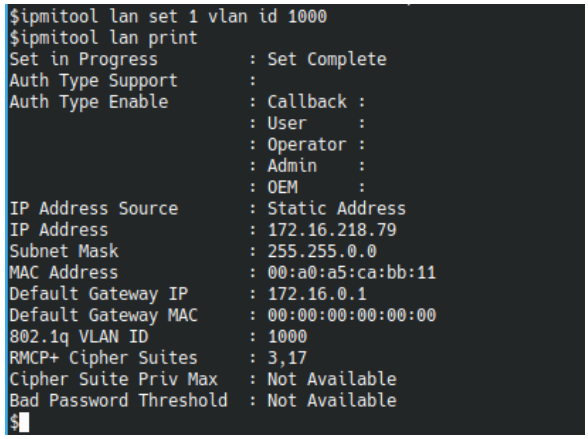
Assigning a VLAN u sing the BMC Web UI

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** .	
Step_2	From the dropdown menu of the **Interface** section, select a network interface to configure.	
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.	
Step_4	Click on **Save settings** .	
Step_5	Configure an IP address for the VLAN interface created using one of the Web UI methods described in this section.	

Assigning a VLAN u sing IPMI

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

Step_1	Associate a pre-configured VLAN to an interface. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] vlan id [VLAN_ID]**	
Step_2	Configure an IP address for the VLAN interface created using one of the IPMI methods described in this section.	

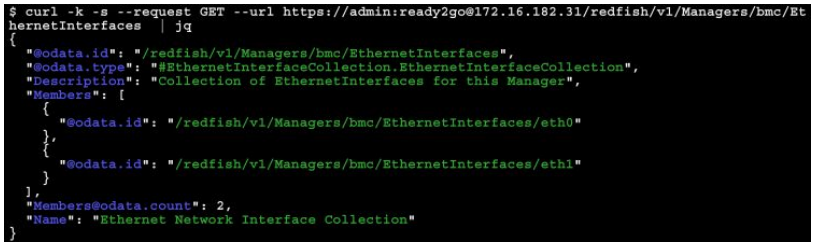
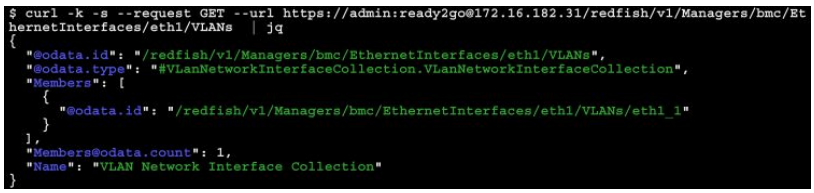
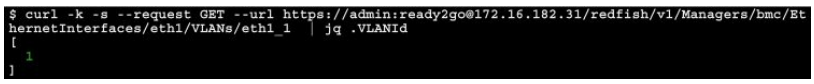
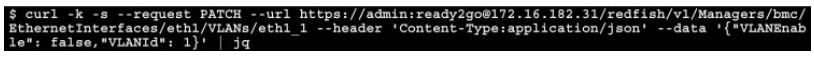
Removing a VLAN

This can be achieved:

- Using Redfish
- Using the BMC Web UI
- Using IPMI

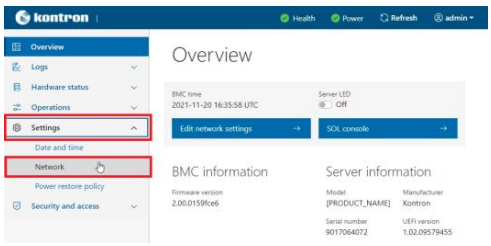
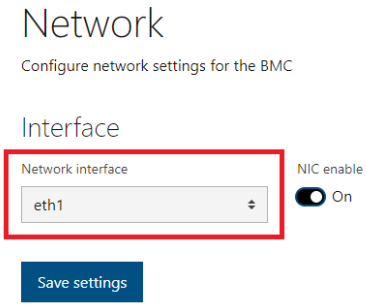
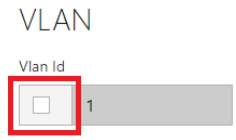
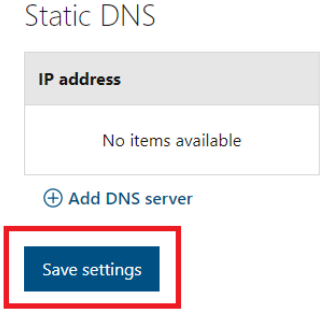
Removing a VLAN using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Select a BMC network interface and take note of its URL. RemoteComputer_OSPrompt:~# curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces | jq
	
Step_2	List the VLANs of a selected BMC network interface and take note of desired VLAN's URL. RemoteComputer_OSPrompt:~# curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces /[INTERFACE_NAME]/VLANs | jq
	
Step_3	Access the VLAN information in order to collect its ID. RemoteComputer_OSPrompt:~# curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]/VLANs/ [VLAN_URL] | jq .VLANId
	
Step_4	Delete the VLAN for the selected BMC network interface using the following command. RemoteComputer_OSPrompt:~# curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]/VLANs/ [VLAN_URL] --header 'Content-Type: application/json' --data '{"VLANEnable": false, "VLANId": [VLAN_ID] }' | jq
	

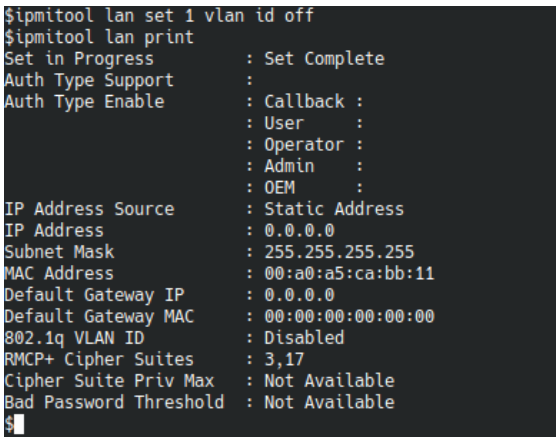
Removing a VLAN using the BMC Web UI

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** .	
Step_2	From the dropdown menu of the **Interface** section, select a network interface to configure.	
Step_3	To remove a VLAN, uncheck the box in the **VLAN** section.	
Step_4	Click on **Save settings** .	

Removing a VLAN using IPMI

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

Step_1	Set the VLAN ID associated with an interface to **off**. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] vlan id off**	

Configuring the integrated server Redfish host interface IP address

Refer to Accessing the operating system of a server for access instructions.
BMC Redfish resources can be accessed locally by the integrated server using the internal, private, Redfish host interface. In this platform, the functionality is implemented using a USB-LAN interface. Most modern Linux operating systems should have built-in support for this USB-LAN device. The procedure below configures the IP address used for the host interface.

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/*/net**
	
	Example in CentOS 7:
	`$ls /sys/bus/usb/drivers/rndis_host/1-3.2:1.0/net`
	`enp0s20f0u3u2`
	`$`
	In this example the interface name discovered is **enp0s20f0u3u2** .
	Example in Ubuntu:
	`$ls /sys/bus/usb/drivers/rndis_host/1-3.2\:1.0/net/`
	`enx00248c46642c`
	`$`
	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]**
	
	`$ip addr add 169.254.0.1/24 dev enp0s20f0u3u2`
	`$ip addr show`
	`1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000`
	`link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00`
	`inet 127.0.0.1/8 scope host lo`
	`valid_lft forever preferred_lft forever`
	`inet6 ::1/128 scope host`
	`valid_lft forever preferred_lft forever`
	`2: eno5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000`
	`link/ether 00:a0:a5:dd:4a:10 brd ff:ff:ff:ff:ff:ff`
	`3: eno4: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000`
	`link/ether 00:00:00:00:03:14 brd ff:ff:ff:ff:ff:ff`
	`4: eno3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000`
	`link/ether 00:00:00:00:03:15 brd ff:ff:ff:ff:ff:ff`
	`5: enp0s20f0u3u2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000`
	`link/ether 00:24:8c:46:64:2c brd ff:ff:ff:ff:ff:ff`
	`inet 169.254.0.1/24 scope global enp0s20f0u3u2`
	`valid_lft forever preferred_lft forever`
	`6: eno2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000`
	`link/ether 00:00:00:00:03:16 brd ff:ff:ff:ff:ff:ff`
	`7: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000`
	`link/ether 00:00:00:00:03:17 brd ff:ff:ff:ff:ff:ff`
	`$_`

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]**
	
	`$curl -k https://admin:ready2go@169.254.0.17/redfish/v1/`
	`{`
	`"@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",`
	`"@odata.id": "/redfish/v1",`
	`"@odata.type": "#ServiceRoot.v1_5_0.ServiceRoot",`
	`"AccountService": {`
	`"@odata.id": "/redfish/v1/AccountService"`
	`},`
	`"CertificateService": {`
	`"@odata.id": "/redfish/v1/CertificateService"`
	`},`
	`"Chassis": {`
	`"@odata.id": "/redfish/v1/Chassis"`
	`},`
	`"Id": "RootService",`
	`"JsonSchemas": {`
	`"@odata.id": "/redfish/v1/JsonSchemas"`
	`},`
	`"Links": {`
	`"Sessions": {`
	`"@odata.id": "/redfish/v1/SessionService/Sessions"`
	`}`
	`},`
	`"Managers": {`
	`"@odata.id": "/redfish/v1/Managers"`
	`},`
	`"Name": "Root Service",`
	`"RedfishVersion": "1.6.1",`
	`"Registries": {`
	`"@odata.id": "/redfish/v1/Registries"`
	`},`
	`"SessionService": {`
	`"@odata.id": "/redfish/v1/SessionService"`
	`},`
	`"Systems": {`
	`"@odata.id": "/redfish/v1/Systems"`
	`},`
	`"UUID": "46e90382-3e10-41f2-b743-a5a850139650",`
	`"UpdateService": {`
	`"@odata.id": "/redfish/v1/UpdateService"`
	`}`
	`}`
	`$`

Configuring UEFI network boot

Table of contents

The following types of network boot options are supported on the platform:

- PXE
- HTTP Boot

UEFI network boot can be configured :

- Using the UEFI/BIOS menu

Configuring UEFI network boot using the UEFI/BIOS menu

Prerequisites

1	Access to the UEFI/BIOS menu is required.
2	A boot server is configured and discoverable using DHCP. **NOTE:** The boot server address cannot be set using a static IP address.

Relevant sections:

Accessing the UEFI or BIOS
Configuring the BMC networking
MAC addresses
PCI mapping
Product architecture

Configuring UEFI networking using the UEFI/BIOS menu

UEFI networking must be configured for the UEFI to communicate with a remote boot server.
NOTE: On a platform with the Ethernet switch IO module, VLANs must be configured for any VLAN-tagged traffic coming from the server E823 25GbE interface.
Refer to Product architecture for information on network interfaces or refer to Configuring VLANs for UEFI network boot for configuration instructions.

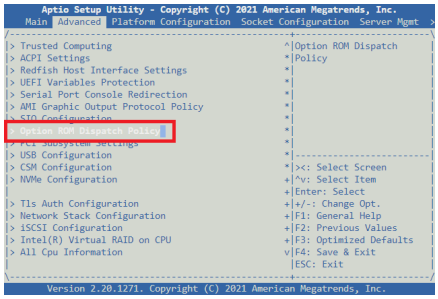
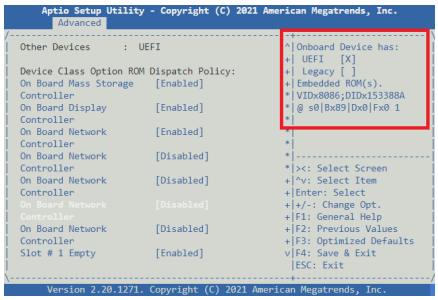
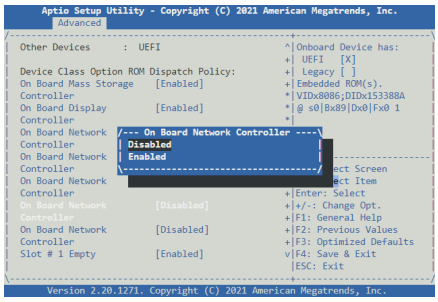
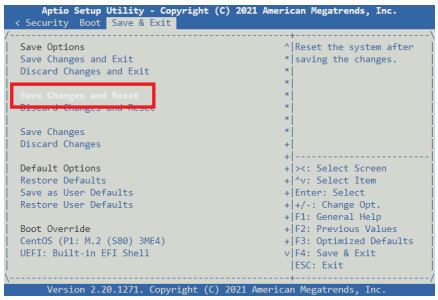
Identifying the network interfaces

At least one UEFI network interface needs to be configured to perform a network boot.
In the UEFI/BIOS menu, the UEFI network interfaces are designated by their PCI mapping. Use the **Bus:Device.Function** column in order to identify the interface in the UEFI/BIOS menu.

Typical designation in Linux	Speed (bps)	NOS port designation	Bus: Device. Function
eno1	25G	Ethernet 1/13	89:00.3
eno2	25G	Ethernet 1/14	89:00.2
eno3	25G	Ethernet 1/15	89:00.1
eno4	25G	Ethernet 1/16	89:00.0
eno5	1G	Not applicable	05:00.0

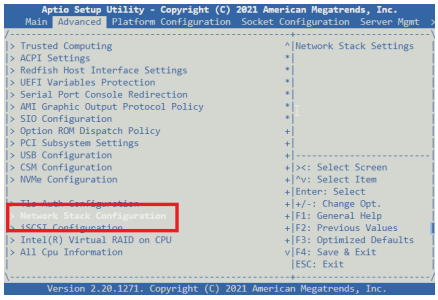
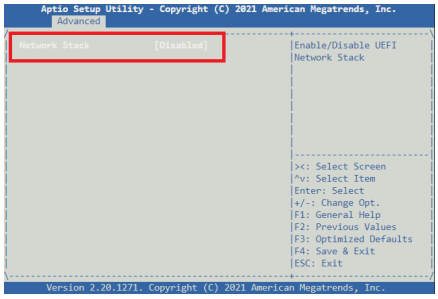
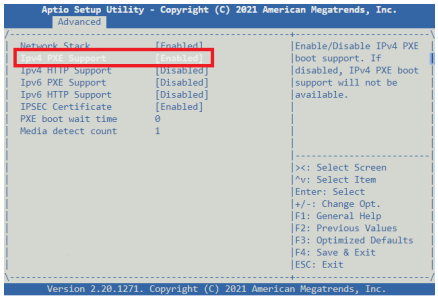
Enabling UEFI support for installed network controllers

Refer to the Identifying the network interfaces table. The help text should match the **Bus:Device.Function** column.

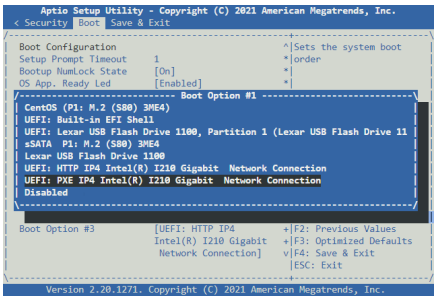
Step_1	Reboot the platform and access the UEFI/BIOS setup menu.	
Step_2	Navigate to the **Advanced** menu and enter the **Option ROM Dispatch Policy** sub-menu.	
Step_3	Identify the network controller using the help text.	
Step_4	Enable or disable the desired network controllers.	
Step_5	Select the **Save & Exit** menu, go to **Save Changes and Reset** and press **Enter** .	

Configuring PXE network boot using the UEFI/BIOS menu

Enabling PXE support

Step_1	From the UEFI/BIOS setup menu, navigate to the **Advanced** menu and enter the **Network Stack Configuration** sub-menu.	
Step_2	If needed, enable the **Network Stack**. **NOTE:** If the network stack is disabled, the UEFI network boot is consequently disabled.	
Step_3	Enable or disable the **IPv4 PXE Support** and/or **IPv6 PXE Support** .	
Step_4	Select the **Save & Exit** menu, go to **Save Changes and Reset** and press **Enter** .	

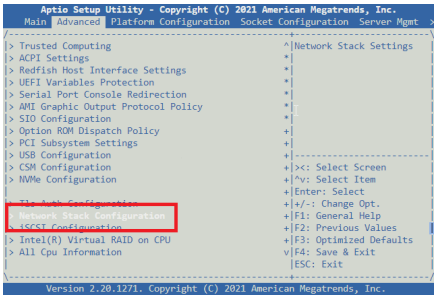
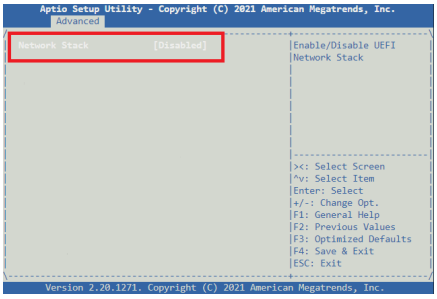
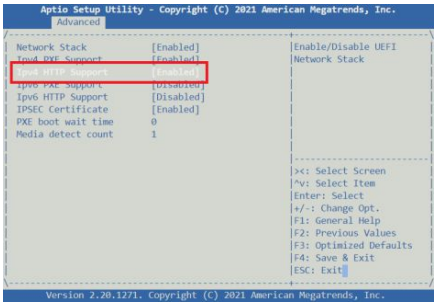
Performing PXE network boot

Step_1	From the UEFI/BIOS setup menu, navigate to the **Boot** menu. Configure the boot order to as desired. The PXE boot option should be first in order to have priority over the other boot options. **NOTE:** Boot override can also be used to choose manually for a one-time boot.	
Step_2	Select the **Save & Exit** menu, go to **Save Changes and Reset** and press **Enter** to confirm and save the new boot order. The platform should boot using PXE.	

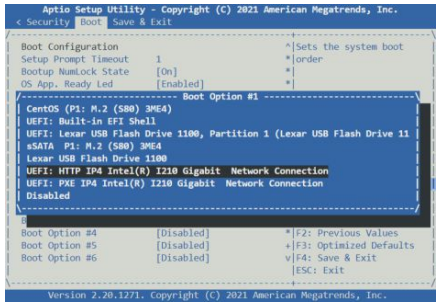
Configuring HTTP network boot using the UEFI/BIOS menu

The **Boot URI** can be set explicitly, but it is very often transmitted by the DHCP server during the IP address selection process. Please consult your network administrator for information pertaining to your installation.

Enabling HTTP boot support

Step_1	From the UEFI/BIOS setup menu, navigate to the **Advanced** menu and enter the **Network Stack Configuration** sub-menu.	
Step_2	If needed, enable the **Network Stack**. **NOTE:** If the network is disabled, the UEFI network boot is consequently disabled.	
Step_3	Enable or disable the **IPv4 HTTP Support** and/or **IPv6 HTTP Support** .	
Step_4	Select the **Save & Exit** menu, go to **Save Changes and Reset** and press **Enter** .	

Performing HTTP network boot

Step_1	Reboot the platform and access the UEFI/BIOS setup menu.	
Step_2	From the UEFI/BIOS setup menu, navigate to the **Boot** menu. Configure the boot order as desired. The HTTP boot option should be first in order to have priority over the other boot options. **NOTE:** Boot override can also be used to choose manually for a one-time boot.	
Step_3	Select the **Save & Exit** menu, go to **Save Changes and Reset** and press **Enter** to confirm and save the new boot order. The platform should boot using HTTP boot.	

Configuring VLANs for UEFI network boot using the UEFI

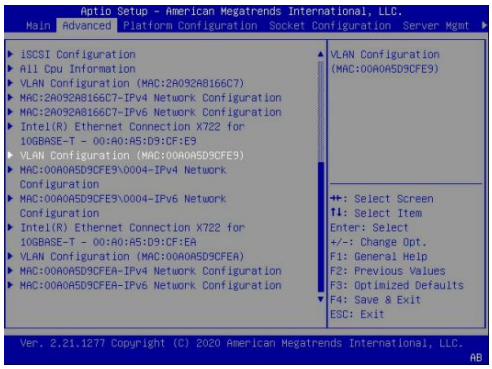
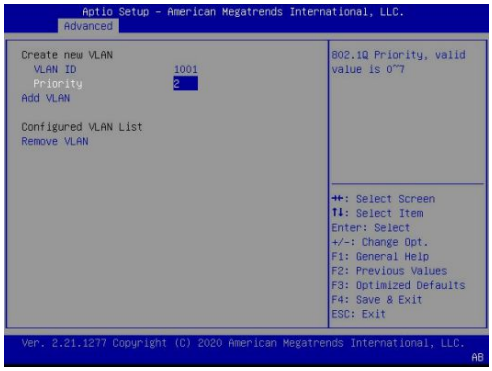
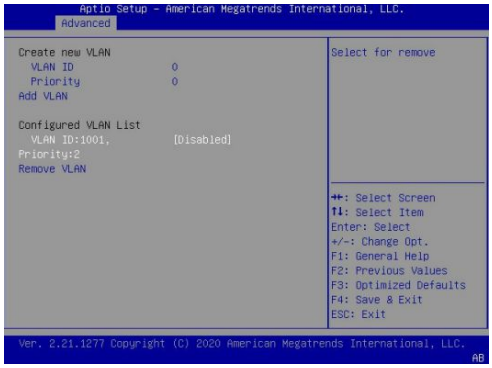
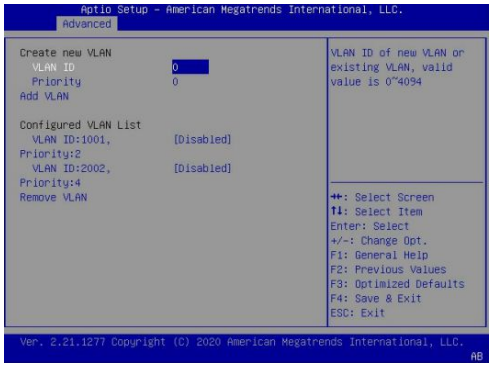
On a platform with the Ethernet switch IO module, VLANs must be configured for any VLAN-tagged traffic coming from the server E823 25GbE interface. Refer to Configuring the switch for procedures to configure VLANs with the switch network operating system.
The UEFI/BIOS setup menu provides options to create/configure/remove VLANs on each of the server's four E823 NIC 25GbE interfaces as well as on the I210 NIC 1GbE interface. Refer to Product architecture for information on network interfaces. However, the UEFI/BIOS setup menus to configure VLANs are available only when the UEFI network services are active.

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

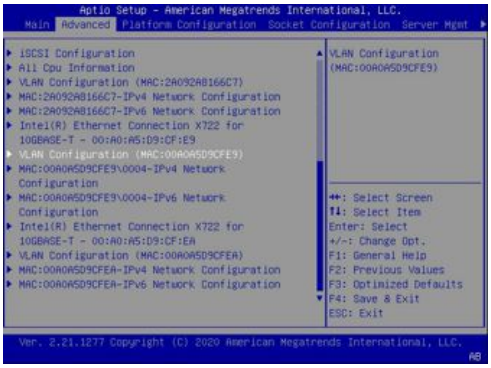
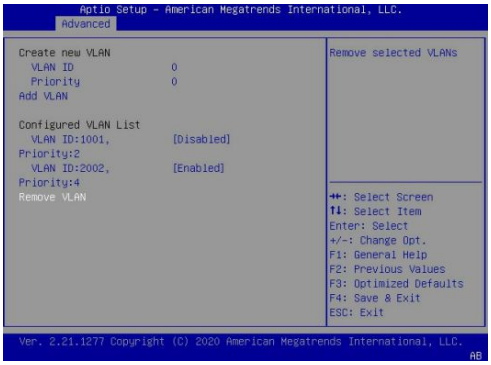
Relevant sections:

- Accessing the UEFI or BIOS
- MAC addresses

Creating VLANs

Step_1	From the UEFI/BIOS setup menu, select the **Advanced** menu and select one **VLAN Configuration (MAC:xxxxxxxxxxxx)** section. Select **Enter Configuration Menu** . **NOTE:** The MAC address will be the MAC address of the E823 25GbE or I210 1GbE interface to configure.	
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.	
Step_3	Select **Add VLAN** to create the VLAN.	
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.	
Step_5	Repeat steps 1 to 4 to assign VLANs for another E823 25GbE interface, as needed.	
Step_6	Press **F4** to save changes and exit.	

Removing VLANs

Step_1	From the UEFI/BIOS setup menu, select the **Advanced** menu and select one **VLAN Configuration (MAC:xxxxxxxxxxxx)** section. Select **Enter Configuration Menu** . **NOTE:** The MAC address will be the one o f the E823 25GbE port for which VLANs must be removed.	
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.	
Step_3	Repeat steps 1 and 2 to remove VLANs in another E823 25GbE interface, as needed.	
Step_4	Press **F4** to save changes and exit.	

Configuring switch NOS networking

Table of contents

Changes to the switch NOS configuration are not persistent after rebooting the switch NOS.
To preserve configurations, the current configuration needs to be saved to startup-config.
From the switch NOS Web UI:

- Select **Maintenance** , **Configuration** and then **Save startup-config** . Click on **Save Configuration** to confirm the change.

From the switch NOS 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

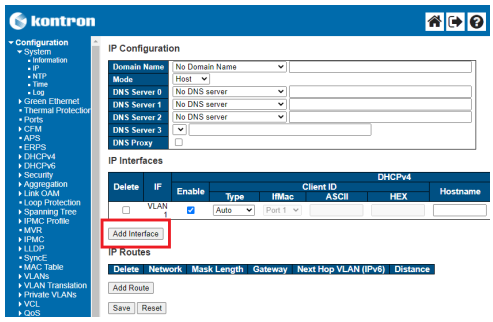
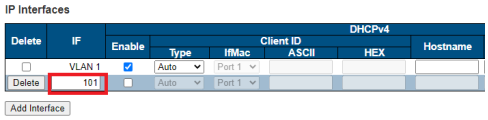
This can be done using:

- The Web UI
- The CLI

Adding 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.

Adding a NOS VLAN interface

Step_1	From the left-side menu, select **Configuration** , **System** and then **IP** .	
Step_2	Click on the **Add Interface** button.	
Step_3	Enter the VLAN numerical ID. **NOTE:** As explained above, the VLAN must already exist to create the NOS IP address interface.	
Step_4	Proceed with IP address configuration as explained below.	

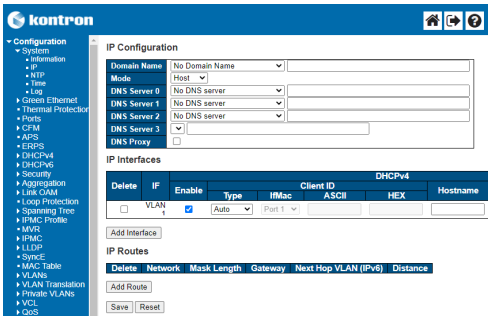
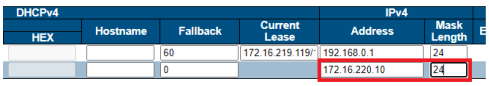
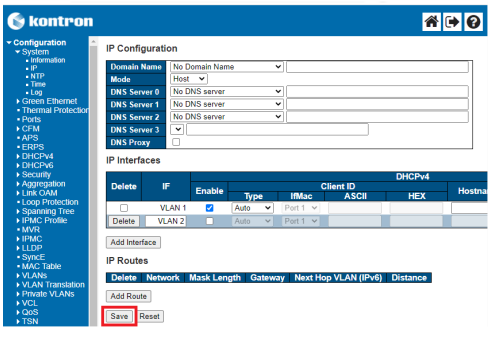
There are two options to configure IP addresses:

- Configuring a static IP address
- Configuring a dynamic IP address using DHCP

Configuring a static IP address

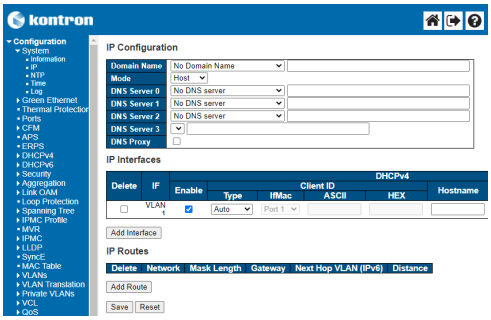
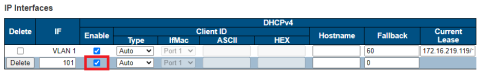
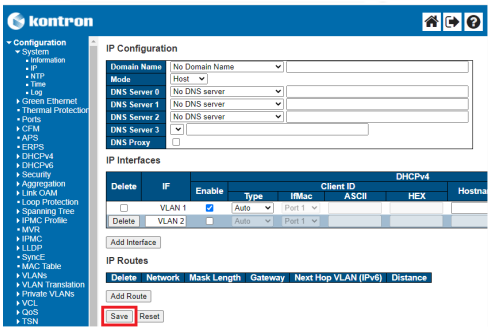
Relevant sections:
Configuring static routing
Configuring DNS

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

Step_1	From the left-side menu, select **Configuration** , **System** and then **IP** .	
Step_2	Manually configure the IP address and the network mask length of the VLAN interface.	
Step_3	Press on the **Save** button to confirm.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring a dynamic IP address using DHCP

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

Step_1	From the left-side menu, select **Configuration** , **System** and then **IP** .	
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.	
Step_3	Press on the **Save** button to confirm.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Adding a NOS VLAN interface IP address using the CLI

Refer to Accessing the switch NOS 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 CLI .

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 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 CLI .

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.	

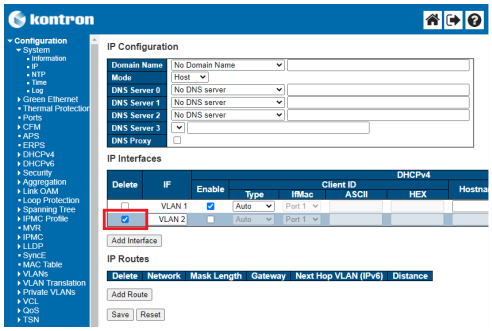
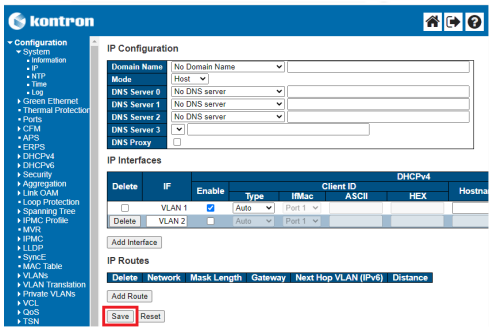
Removing a NOS VLAN interface IP address

This can be done using:

- The Web UI
- The CLI

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 Saving the current configuration using the Web UI .

Step_1	From the left-side menu, select **Configuration** , **System** and then **IP** .	
Step_2	Select the VLAN interface to delete.	
Step_3	Press on the **Save** button to confirm.	
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 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 CLI .

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 HTTPS support

HTTPS support must be configured. This can be done using:

- The switch NOS Web UI
- The switch CLI

Configuring HTTPS support using the Web UI

The Web server can be accessed using two protocols: HTTP and HTTPS. They are independent and both can be used simultaneously. The network switch can therefore operate in any of the following 3 modes:

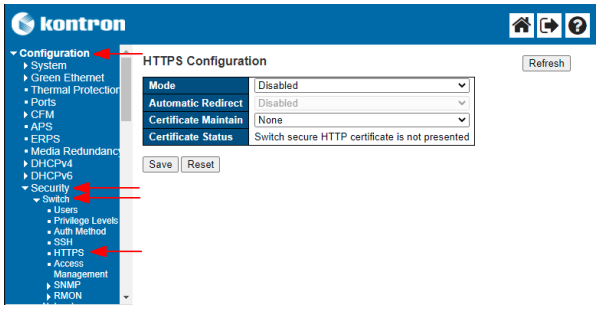
- **HTTP only** – All information is transferred in clear text (even passwords). **Not secure!** Communications are on Port 80.
- **HTTPS only** – All information is transferred in encrypted packets. **Communication is secure** . HTTP requests are automatically translated as HTTPS requests. Communications are on Port 443. **A certificate is required for HTTPS.**
- **HTTP and HTTPS** – Users can use any of the 2 protocols. **This is the default state, but a certificate is required for HTTPS.**

For the secure HTTPS protocol to work, a certificate needs to be installed . See the Certificates section below.

HTTPS configuration page

Refer to Accessing the switch NOS using the switch NOS Web UI for access instructions.
This page is used to configure the HTTPS settings and maintain the current certificate on the switch.

i	For the secure HTTPS protocol to work, a certificate needs to be installed. As a temporary measure, the switch can create a self-signed certificate, which is secure but cannot be trusted as a long term solution. Users will need to provide their own certificate, delivered from a valid certificate authority.

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **HTTPS** .	
Step_2	Select the desired settings for **Mode** , **Automatic Redirect** , **Certificate Maintain** (based on the value chosen, additional fields will be available) and **Certificate Status** . See the table below for an explanation of the values available for each field.	
Step_3	Press on the **Save** button to confirm.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Values available for fields used for HTTPS configuration

Field			Description	Values
Mode			Sets the HTTPS operation mode.	**Enabled** : HTTPS operation mode is enabled. **Disabled** : HTTPS operation mode is disabled.
Automatic Redirect			Sets the HTTPS redirect operation mode. This setting is required only when **Mode** is set to **Enabled** . When redirection is enabled, the HTTP connection will be redirected to the HTTPS connection automatically. Note that the browser may not allow redirection due to security considerations, unless the switch certificate is trusted by the browser. An HTTPS connection needs to be manually initialized in this case. When the value of this field is set to **Enabled** , the HTTP protocol is effectively disabled.	**Enabled** : HTTPS redirect operation mode is enabled. **Disabled** : HTTPS redirect operation mode is disabled.
Certificate Maintain			Performs certificate maintenance. This setting is operational only when **Mode** is set to **Disabled** .	**None** : Nothing happens. **Delete** : Deletes the current certificate. **Upload** : Uploads a certificate PEM file. **Generate** : Generates a new self-signed RSA certificate.
	Certificate Pass Phrase (Available when the **Certificate Maintain** field is set to **Upload** .)		Holds the passphrase protecting the certificate to upload.	
	Certificate Upload (Available when the **Certificate Maintain** field is set to **Upload** .)		Uploads a certificate PEM file into the switch. The file should contain both the certificate and private key. If the certificate and private key are in	**Web Browser** : Upload a certificate via a Web browser. **URL** : Upload a certificate via an URL.

			two separate files, use the Linux cat command to combine them into a single PEM file: `cat my.cert my.key > my.pem` Note that an RSA certificate is recommended since most newer browser versions have removed support for DSA in certificates (e.g. Firefox v37 and Chrome v39).	
		File Upload (Available when the **Certificate Upload** field is set to **Web Browser** .)	Lets users select the file to upload.	
		URL (Available when the **Certificate Upload** field is set to **URL** .)	Holds the URL.	URL format: [PROTOCOL]://[USERNAME]:[PASSWORD]@[HOST_IP_ADDRESS]:[PORT] [FILE_PATH] . The protocols supported are HTTP, HTTPS, TFTP and FTP. For example: • **tftp://10.10.10.10/new_image_path/new_image.dat** • http://username:password@10.10.10.10:80/new_image_path/new_image.dat A valid file name is a text string drawn from alphabet letters (A-Za-z), digits (0-9), dots (.), hyphens (-) and under scores (_). The maximum length is 63 and a hyphen must not be the first character. A file name that only contains '.' is not allowed.
Certificate Status			Displays the current status of the switch certificate.	**Switch secure HTTP certificate is presented :** When a valid certificate is present. **Switch secure HTTP certificate is not presented :** When no valid certificate is present or the certificate has been deleted. **Switch secure HTTP certificate is generating ....:** When the self-signed certificate is being generated (wait 1 minute and then refresh the page for results).

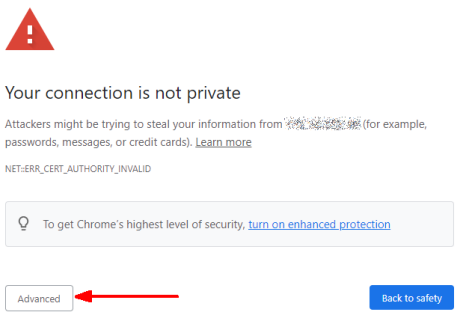
Certificates

Refer to Accessing the switch NOS using the switch NOS Web UI for access instructions.
Any certificate will allow the web server to encrypt the information transferred.
Only certificates obtained from a trusted Certificate Authority (CA) can guarantee authenticity trough a chain of thrust. CA User Certificate Platform certificate.
There are 3 ways to insert a certificate:

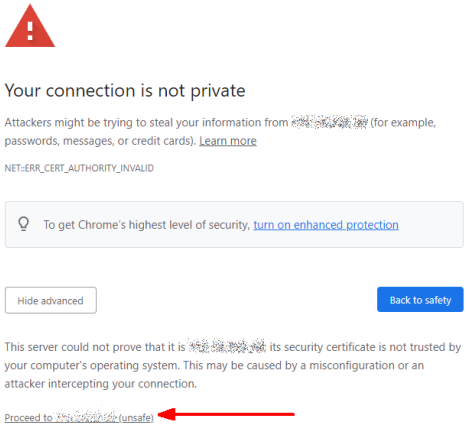
- **Generate a self-signed certificate** – this should only be a temporary solution. It is secure, but not safe. Data will be encrypted, but cannot be trusted.
- **Upload a certificate from a URL**
- **Upload a certificate from a user file system**

Generating a self-signed certificate

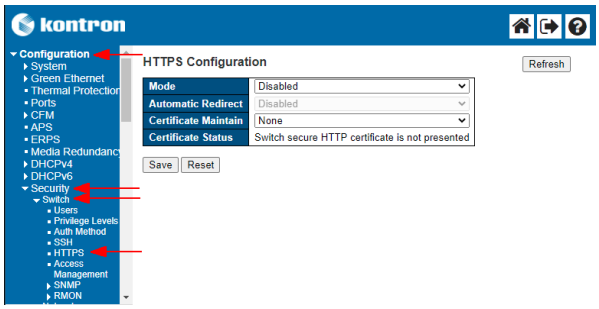
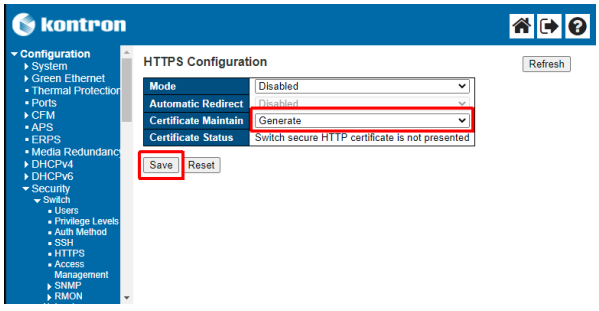
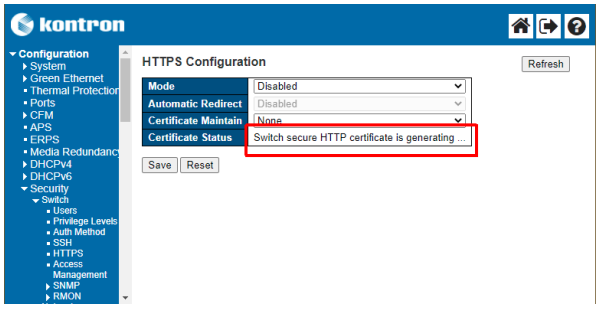
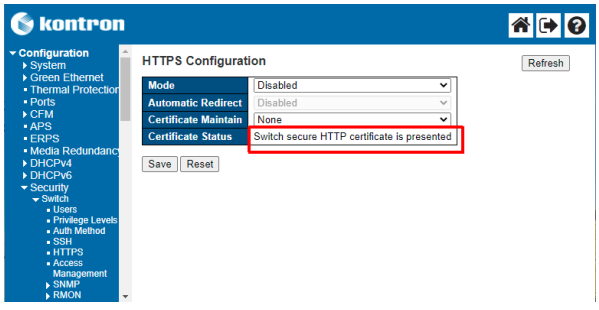
A self-signed certificate, which should only be used as a temporary solution, allows communication to be encrypted, but cannot certify that the server is really what it claims to be.
NOTE : The self-signed certificate will be valid for a fixed time period (e.g. November 30th 2021 at 00:00:01 up to November 30th 2031 at 23:59:59).
If a self-signed certificate is used, the Web browser will display a warning message before you can access the page. If this is the case, click on **Advanced.**



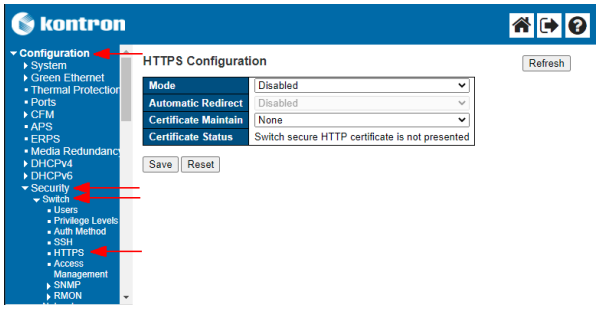
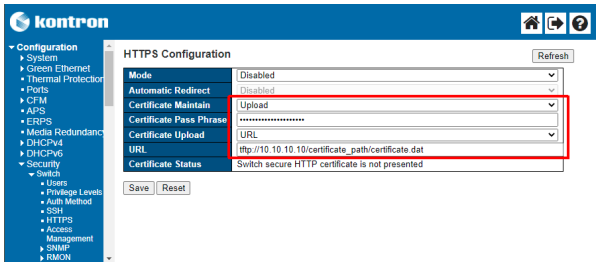
Then click on the **Proceed to [IP_ADDRESS] (unsafe)** link.



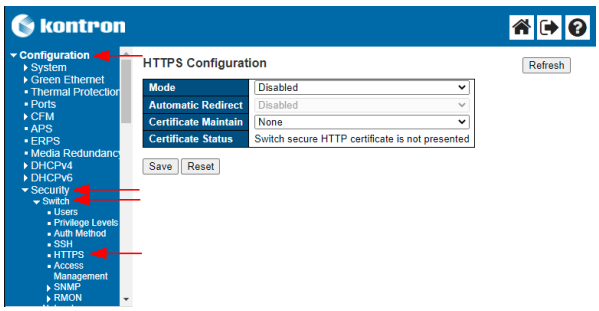
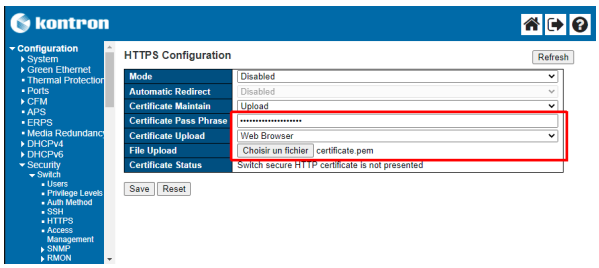
From the switch Web UI, perform the following steps.

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **HTTPS** .	
Step_2	Set the **Certificate Maintain** field to **Generate** .	
Step_3	Press **Save** to confirm.	
Step_4	The **Certificate Status** field will indicate that the switch is generating the certificate and will self-refresh.	
Step_5	The **Certificate Status** field will indicate that the certificate is present.	
Step_6	(Optional) To make the change persistent, save running-config to startup-config.	

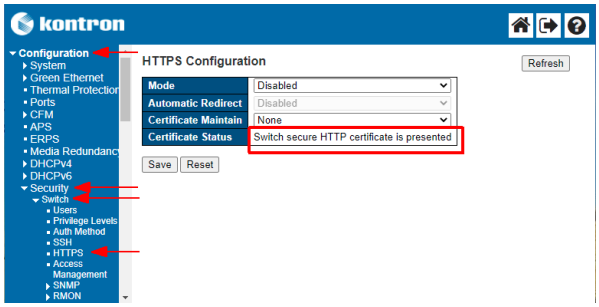
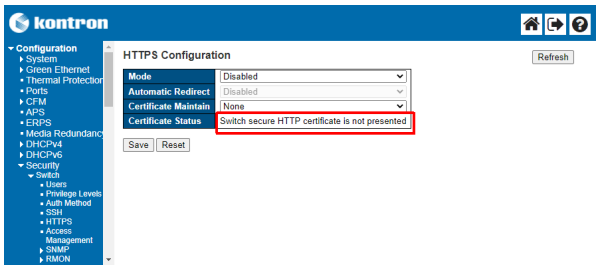
Uploading a certificate from a URL

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **HTTPS** .	
Step_2	Set the **Certificate Maintain** field to **Upload** .	
Step_3	Enter the pass phrase in the **Certificat Pass Phrase** field.	
Step_4	Set the **Certificate Upload** field to **URL** .	
Step_5	Enter the URL of the certificate in field **URL**.	
Step_6	Press **Save** to confirm.	
Step_7	The **Certificate Status** field will indicate that the certificate is present.	
Step_8	(Optional) To make the change persistent, save running-config to startup-config.	

Uploading a certificate from a user file system

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **HTTPS** .	
Step_2	Set the **Certificate Maintain** field to **Upload** .	
Step_3	Enter the pass phrase in the **Certificat Pass Phrase** field.	
Step_4	Set the **Certificate Upload** field to **Web Browser** .	
Step_5	In the **File Upload** field, click **Choose a file** and browse for the desired file.	
Step_6	Press **Save** to confirm.	
Step_7	The **Certificate Status** field will indicate that the certificate is in present.	
Step_8	(Optional) To make the change persistent, save running-config to startup-config.	

Deleting an installed certificate

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **HTTPS** . Ensure the **Certificate Status** is set to **Switch secure HTTP certificate is presented** .	
Step_2	Set the **Certificate Maintain** field to **Delete** .	
Step_3	The **Certificate Status** field will indicate that the **Switch secure HTTP certificate is not presented** .	
Step_4	Press **Save** to confirm.	
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

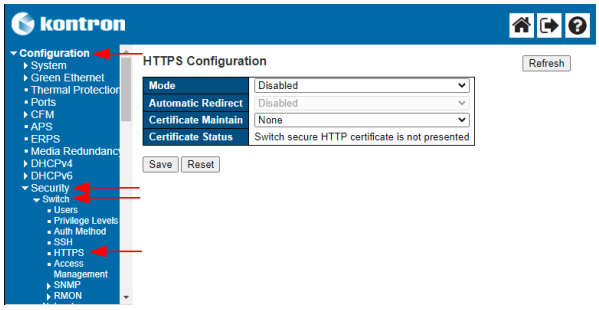
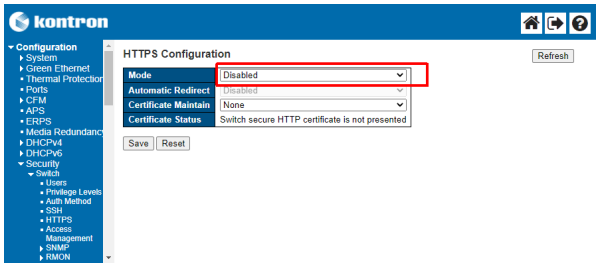
Configuring the interface protocol

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

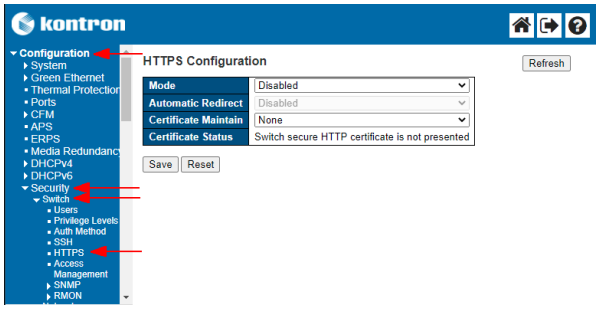
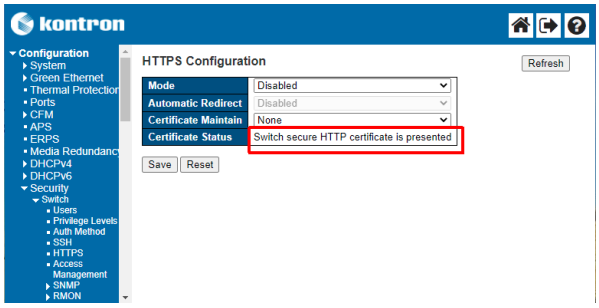
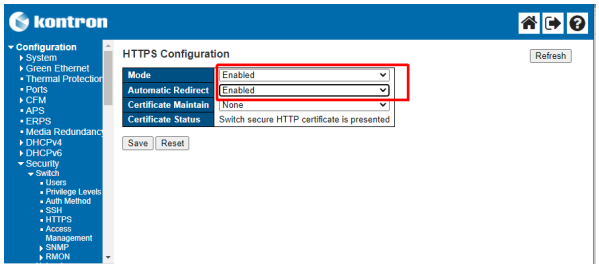
Th ere are three options to configure the interface protocol:

- HTTP only
- HTTPS only
- HTTP and HTTPS

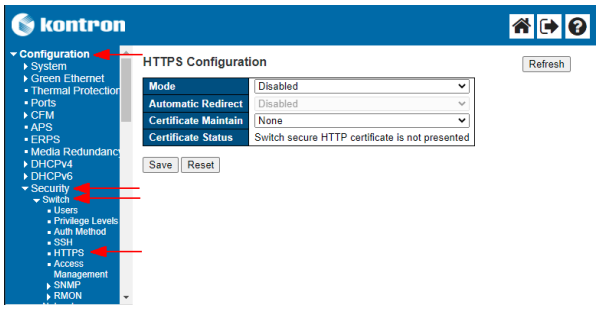
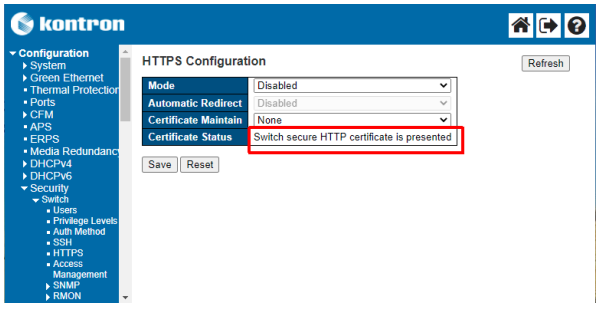
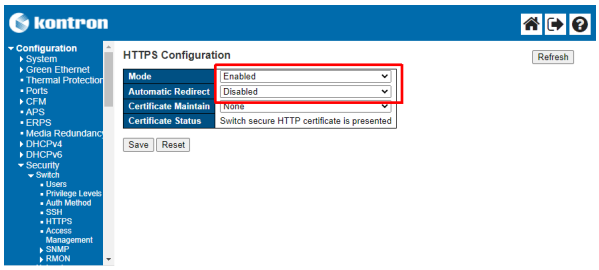
Configuring the interface for HTTP only

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **HTTPS** .	
Step_2	Set the **Mode** field to **Disabled** .	
Step_3	Press **Save** to confirm.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the interface for HTTPS only

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **HTTPS** .	
Step_2	Ensure the **Certificate Status** field is set to **Switch secure HTTP certificate is presented** .	
Step_3	Set the **Mode** field to **Enabled** .	
Step_4	Set the **Automatic Redirect** field to **Enabled** .	
Step_5	Press **Save** to confirm.	
Step_6	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the interface for HTTP and HTTPS

Step_1	From the left-side menu, select **Configuration** , **Security** , **Switch** and then **HTTPS** .	
Step_2	Ensure the **Certificate Status** field is set to **Switch secure HTTP certificate is presented** .	
Step_3	Set the **Mode** field to **Enabled** .	
Step_4	Set the **Automatic Redirect** field to **Disabled** .	
Step_5	Press **Save** to confirm.	
Step_6	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring HTTPS support using the CLI

The Web server can be accessed using two protocols: HTTP and HTTPS. They are independent and both can be used simultaneously. The network switch can therefore operate in any of the following 3 modes:

- **HTTP only** – All information is transferred in clear text (even passwords). **Not secure!** Communications are on Port 80.
- **HTTPS only** – All information is transferred in encrypted packets. **Communication is secure** . HTTP requests are automatically translated as HTTPS requests. Communications are on Port 443. **A certificate is required for HTTPS.**
- **HTTP and HTTPS** – Users can use any of the 2 protocols. **This is the default state, but a certificate is required for HTTPS.**

For the secure HTTPS protocol to work, a certificate needs to be installed . See the Certificates section below.

Displaying HTTP and HTTPS states

Refer to Accessing the switch network operating system for access instructions.
To know the states of the various secure HTTP variables, two command can be used: **show ip http** (in normal mode) or **do show ip http** (in configuration mode).

Step_1	LocalSwitchNOS_OSPrompt:~# **show ip http**	NOS00A0A5E01CF4# show ip http Switch secure HTTP web server is disabled Switch secure HTTP web redirection is disabled Switch secure HTTP certificate is not presented

Field	Description	Value
Switch secure HTTP web server is	Shows the state of the **Switch secure HTTP web server** . When the state is **Enabled** , secure HTTPS communications trough port 443 are available. **NOTE** : For the state to be **Enabled** , a certificate **must** be present.	Enabled Disabled
Switch secure HTTP web redirection is	When the state is **Enabled** , HTTP communications are redirected to the **Switch secure HTTP web server** . This means the HTTP web server is no longer used. **NOTE** : For the state to be **Enabled** , the **Switch secure HTTP web server must** be set to **Enabled** beforehand.	Enabled Disabled
Switch secure HTTP certificate is	Shows if a certificate is installed in the system. Presented means that a certificate is installed and can be used for HTTPS encryption.	Presented Not presented

Certificates

Refer to Accessing the switch network operating system for access instructions.
Any certificate will allow the web server to encrypt the information transferred.
Only certificates obtained from a trusted Certificate Authority (CA) can guarantee authenticity trough a chain of thrust. CA User Certificate Platform certificate.
There are 3 ways to insert a certificate:

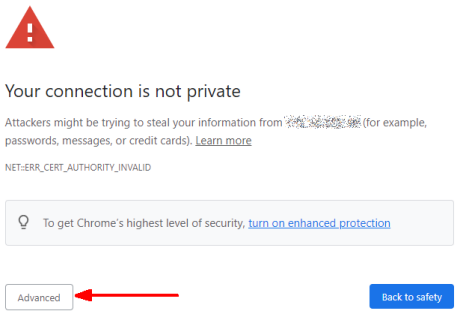
- **Generate a self-signed certificate** – this should only be a temporary solution. It is secure, but not safe. Data will be encrypted, but cannot be trusted.
- **Upload a certificate from a URL**
- **Upload a certificate from a user file system**

Displaying available commands

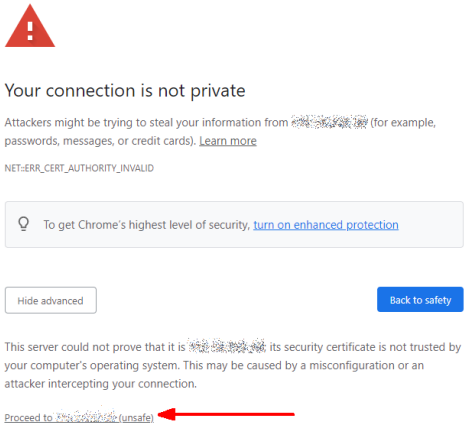
Step_1	Go in configuration mode. LocalSwitchNOS_OSPrompt:~# **configure terminal**	NOS00A0A5E01CF4# configure terminal NOS00A0A5E01CF4(config)# ip http secure-certificate ? delete Delete the current certificate generate Generate a new self-signed RSA certificate upload Upload a certificate PEM file
Step_2	Show available commands. LocalSwitchNOS_OSPrompt:~(config)# **ip http secure-certificate ?**	

Generating a self-signed certificate

A self-signed certificate, which should only be used as a temporary solution, allows communication to be encrypted, but cannot certify that the server is really what it claims to be.
NOTE : The self-signed certificate will be valid for a fixed time period (e.g. November 30th 2021 at 00:00:01 up to November 30th 2031 at 23:59:59).
If a self-signed certificate is used, the Web browser will display a warning message before you can access the page. If this is the case, click on **Advanced.**



Then click on the **Proceed to [IP_ADDRESS] (unsafe)** link.



From the network switch CLI:

Step_1	Go in configuration mode. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`NOS00A0A5E01CF4# configure terminal` `NOS00A0A5E01CF4(config)# ip http secure-certificate generate`
Step_2	Generate a certificate. LocalSwitchNOS_OSPrompt:~(config)# **ip http secure-certificate generate**	

Step_3	Ensure the certificate and HTTP web server are correctly configured.
	LocalSwitchNOS_OSPrompt:~# **do show ip http**
	NOTE : Certificate generation can take a few seconds. If it is still generating when checking the status, the CLI will indicate that it is generating...
		`NOS00A0A5E01CF4(config)# do show ip http`
		`Switch secure HTTP web server is disabled`
		`Switch secure HTTP web redirection is disabled`
		`Switch secure HTTP certificate is generating ...`

Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Uploading a certificate from a URL

Step_1	Enter the configuration terminal. LocalSwitchNOS_OSPrompt:~# **configure terminal**

Step_2	Upload the certificate.
	LocalSwitchNOS_OSPrompt:~(config)# **ip http secure-certificate upload [PROTOCOL] ://[USERNAME]: [PASSWORD]@ [HOST_IP_ADDRESS]: [PORT][FILE_PATH]**
	`NOS00A0A5E01CF4# configure terminal`
	`NOS00A0A5E01CF4(config)# ip http secure-certificate upload tftp://10.10.10.10/certificate.pem`

Step_3	Ensure the certificate and HTTP web server are correctly configured.
	LocalSwitchNOS_OSPrompt:~# **do show ip http**
	NOTE : Certificate generation can take a few seconds. If it is still generating when checking the status, the CLI will indicate that it is generating.
	`NOS00A0A5E01CF4(config)# do show ip http`
	`Switch secure HTTP web server is disabled`
	`Switch secure HTTP web redirection is disabled`
	`Switch secure HTTP certificate is generating ...`

Step_4	(Optional) To make the change persistent, save running-config to startup-config.

Deleting an installed certificate

Step_1	Go in configuration mode.
	LocalSwitchNOS_OSPrompt:~# **configure terminal**
		`NOS00A0A5E01CF4# configure terminal`
		`NOS00A0A5E01CF4(config)# ip http secure-certificate delete`
		`NOS00A0A5E01CF4(config)#`

Step_2	LocalSwitchNOS_OSPrompt:~(config)# **ip http secure-certificate delete**	
Step_3	Ensure the certificate and HTTP web server are correctly configured. LocalSwitchNOS_OSPrompt:~# **do show ip http**	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the interface protocol

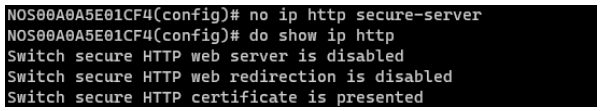
Refer to Accessing the switch network operating system for access instructions.

There are three options to configure the interface protocol:

- HTTP only
- HTTPS only
- HTTP and HTTPS

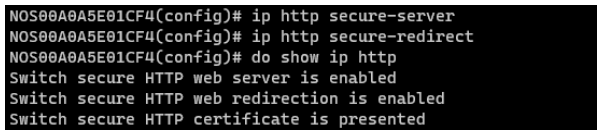
Configuring the interface for HTTP only

If the interface is configured for HTTP only, the HTTPS Switch secure HTTP web server will be disabled and so will the Switch secure HTTP web redirection.

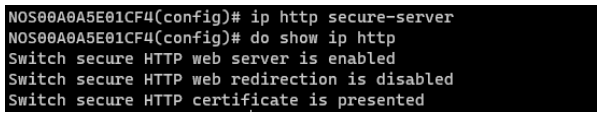
Step_1	Enter the configuration terminal. LocalSwitchNOS_OSPrompt:~# **configure terminal**	
Step_2	LocalSwitchNOS_OSPrompt:~(config)# **no ip http secure-server**	
Step_3	Ensure the certificate and HTTP web server are correctly configured. LocalSwitchNOS_OSPrompt: ~(config) # **do show ip http**	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the interface for HTTPS only

To configure the interface for HTTPS only, the HTTPS server must be enabled and the redirection must also be enabled. This will disable the HTTP server.

Step_1	Enter the configuration terminal. LocalSwitchNOS_OSPrompt:~# **configure terminal**	
Step_2	Configure the interface for HTTPS. LocalSwitchNOS_OSPrompt:~(config)# **ip http secure-server**	
Step_3	Enable redirection. LocalSwitchNOS_OSPrompt:~(config)# **ip http secure-redirect**	
Step_4	Ensure the certificate and HTTP web server are correctly configured. LocalSwitchNOS_OSPrompt: ~(config) # **do show ip http**	
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the interface for HTTP and HTTPS

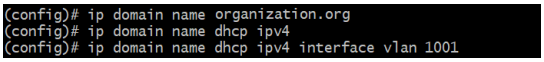
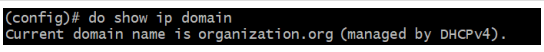
Step_1	Enter the configuration terminal. LocalSwitchNOS_OSPrompt:~# **configure terminal**	
Step_2	LocalSwitchNOS_OSPrompt:~(config)# **ip http secure-server**	
Step_3	Ensure the certificate and HTTP web server are correctly configured. LocalSwitchNOS_OSPrompt: ~(config) # **do show ip http**	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring DNS

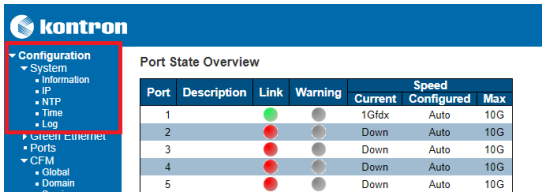
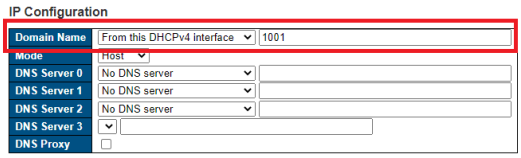
NOTE: Only IPv4-based protocols have been tested and therefore no IPv6 protocols have been documented.

Configuring the domain name

Configuring the domain name using the CLI

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# **configure terminal**	
Step_2	Three methods of domain name configuration are supported. A server can be configured from a local domain name, from any DHCPv4-enabled VLAN interface, or from a specific DHCPv4-enabled VLAN interface. The following examples cover all methods. LocalSwitchNOS_OSPrompt:~# **ip domain name [DOMAIN_NAME]** LocalSwitchNOS_OSPrompt:~# **ip domain name dhcp ipv4** LocalSwitchNOS_OSPrompt:~# **ip domain name dhcp ipv4 interface vlan [VLAN_ID]** To disable the domain name, use the **no** prefix before the **domain name** command. LocalSwitchNOS_OSPrompt:~# **no ip domain name**	
Step_3	Verify that configuration was successful. LocalSwitchNOS_OSPrompt:~# **do show ip domain**	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the domain name using the Web UI

Step_1	From the left-side menu, select **Configuration**, then **System** and then **IP** .	
Step_2	From the **IP Configuration** section, select the **Domain Name** configuration method from the dropdown menu. Then, if required, configure the value in the adjacent input field. The configuration methods are as listed below: • **No Domain Name:** No domain name will be used. No value is required in the input field. • **Configured Domain Name:** Explicitly specify the name of the local domain in the input field. Make sure the configured domain name meets your organization's given domain. • **From any DHCPv4 interfaces:** The first domain name offered from a DHCPv4 lease to a DHCPv4-enabled VLAN interface will be used. No value is required in the input field. • **From this DHCPv4 interface:** Specify from which DHCPv4-enabled VLAN interface a provided domain name should be preferred.	Example for **Configured Domain Name:**  Example for **From this DHCPv4 Interface** : 
Step_3	Click on the **Save** button.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring a DNS server

Configuring a DNS server using the CLI

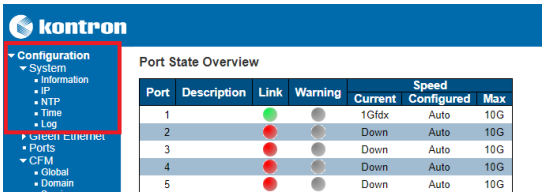
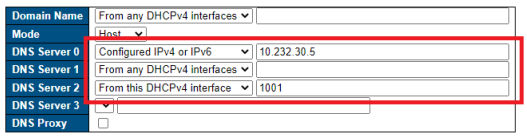
Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`

Step_2	Up to 3 DNS servers can be configured in the switch NOS. The DNS server IDs can range from 0 to 2.
	Three methods of DNS server configuration are supported. A server can be configured from a DNS server IPv4 unicast address, from any DHCPv4-enabled VLAN interface, or from a specific DHCPv4-enabled VLAN interface. The following examples cover all methods.
	LocalSwitchNOS_OSPrompt:~# **ip name-server [DNS_SERVER _ID] [DNS_SERVER _ IP_ADDR]**
	LocalSwitchNOS_OSPrompt:~# **ip name-server [DNS_SERVER _ID] dhcp ipv4**
	LocalSwitchNOS_OSPrompt:~# **ip name-server [DNS_SERVER _ID] dhcp ipv4 interface vlan [VLAN_ID]**
	
	To disable a DNS server, use the **no** prefix before the **name-server** command.
	LocalSwitchNOS_OSPrompt:~# **no ip name-server [DNS_SERVER _ID]**
		`(config)# ip name-server 0 10.232.30.5`
		`(config)# ip name-server 1 dhcp ipv4`
		`(config)# ip name-server 2 dhcp ipv4 interface vlan 1001`

Step_3	Verify that configuration was successful.
	LocalSwitchNOS_OSPrompt:~# **do show ip name-server**
		`(config)# do show ip name-server`
		
		`Configured DNS server 0 is set by NONE:`
		`No address is used for DNS lookup.`
		`Configured DNS server 1 is set by DHCPv4 VLAN 1:`
		`10.232.30.5 is used for DNS lookup on IP VLAN 1.`
		`Configured DNS server 2 is set by DHCPv4 VLAN 1001:`
		`No address is used for DNS lookup on IP VLAN 1001.`

Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring a DNS server using the Web UI

Step_1	From the left-side menu, select **Configuration**, then **System** and then **IP** .	
Step_2	From the **IP Configuration** section, se lect the DNS server conf iguration method from the dropdown menu. Then, if required, configure the value in the adjacent input field. The configuration methods are as listed below: • **No DNS server**: No DNS server will be used. • **Configured IPv4**: Explicitly provide the IPv4 unicast address of the DNS server in dotted decimal notation in the input field. Make sure the configured DNS server is reachable. • **From any DHCPv4 interfaces**: The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used. • **From this DHCPv4 interface**: Specify from which DHCPv4-enabled interface a provided DNS server should be preferred. Enter a VLAN ID in the input field.	
Step_3	Click on the **Save** button.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring proxy DNS

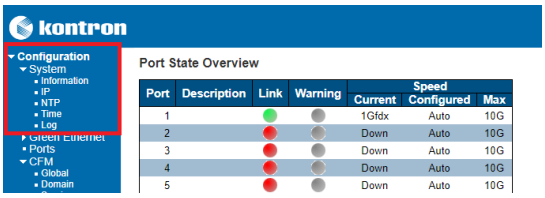
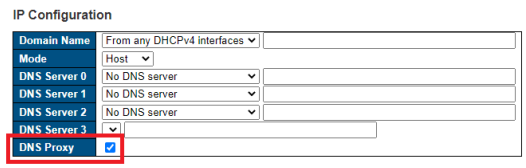
Configuring proxy DNS using the CLI

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`

Step_2	To enable the proxy DNS, use the following command.
	LocalSwitchNOS_OSPrompt:~(config)# **ip dns proxy**
	To disable the proxy DNS, use the same command with the no prefix.
	LocalSwitchNOS_OSPrompt:~(config)# **no ip dns proxy**
		`(config)# ip dns proxy`
		`(config)#`
		
		`(config)# no ip dns proxy`
		`(config)#`

Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Enabling proxy DNS using the Web UI

Step_1	From the left-side menu, select **Configuration**, then **System** and then **IP** .	
Step_2	From the **IP Configuration** , enable or disable proxy DNS by clicking on the **DNS Proxy** checkbox.	
Step_3	Click on the **Save** button.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring BMC services

Configuring BMC SNMP

Table of contents

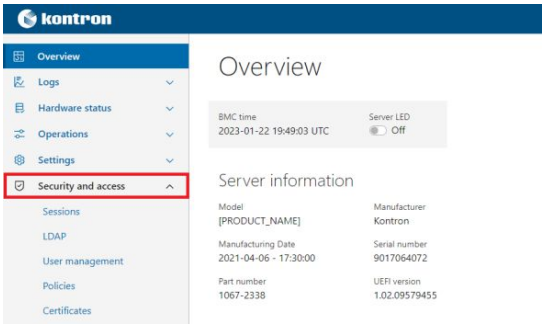
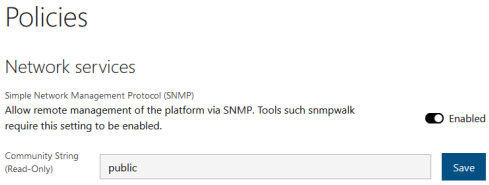
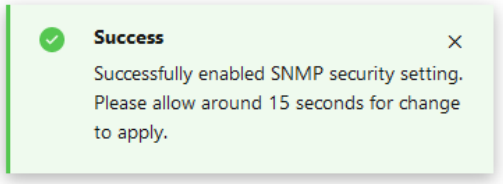
Configuring SNMP remote management

The BMC SNMP can be configured:

- Using the BMC Web UI
- Using Redfish

Configuring SNMP remote management 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, select **Security and access** and then **Policies** .	
Step_2	Enable or disable SNMP remote management using the radio button.	
Step_3	If SNMP remote management was enabled, change the Community String to a unique name.	
Step_4	Click on the **Save** button.	
Step_5	A success message should appear upon successful configuration.	

Configuring SNMP remote management using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	**Enable** or **Disable** SNMP remote management using the following command. Possible values for [ENABLED] are: • **true** • **false** RemoteComputer_OSPrompt:~$ **curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '{"SNMP":{"ProtocolEnabled":[ENABLED]}}' | jq**
	`curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '{"SNMP":{"ProtocolEnabled":true}}' | jq`
Step_2	Configure SNMP remote management **Community String**. Ensure that **[STRING]** is a unique community name. RemoteComputer_OSPrompt:~$ **curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '{"CommunityString":"[STRING]"}' | jq**
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '{"CommunityString":"communitystring"}' | jq`

Configuring BMC event subscriptions

Table of contents

Relevant section :
Configuring BMC SNMP

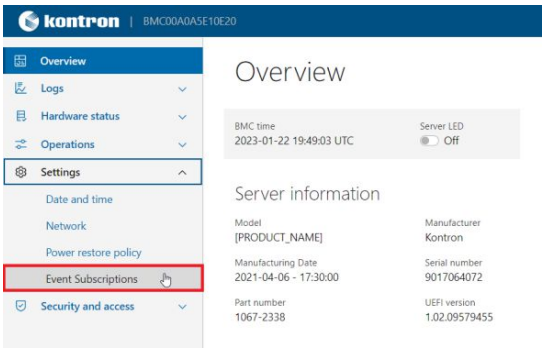
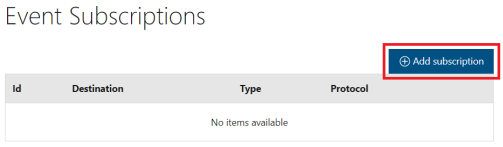
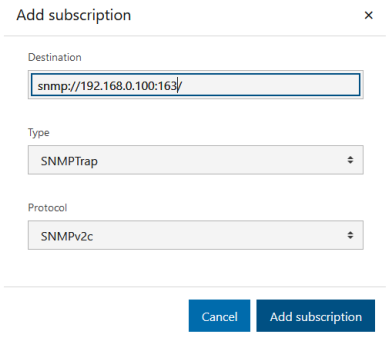
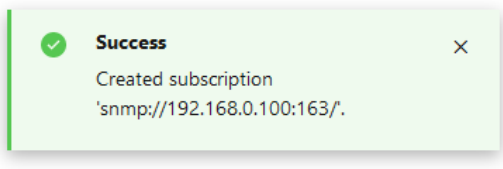
Configuring the SNMP traps

The BMC SNMP traps can be configured:

- Using the BMC Web UI
- Using Redfish

Configuring the SNMP traps 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, select **Settings** and then **Event Subscriptions** .	
Step_2	Click on the **Add subscription** button.	
Step_3	In the **Add subscription** menu, enter the destination address into the **Destination** field. The destination address should be formatted as follows: **[PROTOCOL]://[ADDRESS]:[PORT]/** **NOTE:** The slash (/) at the end of the destination address is required.	
Step_4	Select **SNMPTrap** from the **Type** dropdown menu.	
Step_5	Select **SNMPv2c** from the **Protocol** dropdown menu.	
Step_6	A success message should appear in the top right corner upon successful configuration.	

Configuring the SNMP traps using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Add a new SNMP trap **subscription** using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request POST --url [ROOT_URL]/redfish/v1/EventService/Subscriptions --header 'Content-Type: application/json' --data '{"Destination": "snmp://[SERVER]:[PORT]", "SubscriptionType": "SNMPTrap", "Protocol": "SNMPv2c"}' | jq**

```
curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/EventService/Subscriptions --header 'Content-Type: application/json' --data '{"Destination": "snmp://192.168.0.1:163","SubscriptionType": "SNMPTrap","Protocol": "SNMPv2c"}' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "The resource has been created successfully",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Created",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

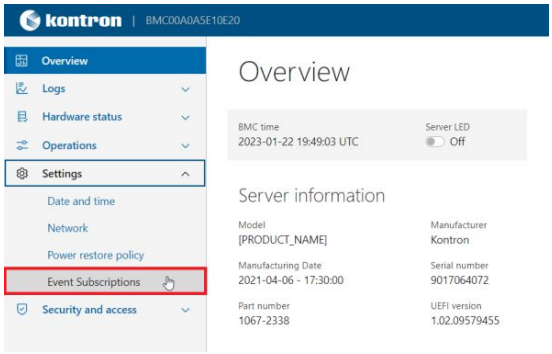
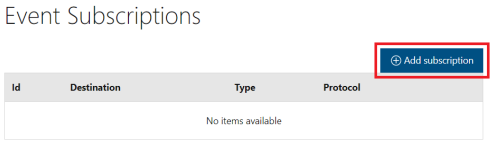
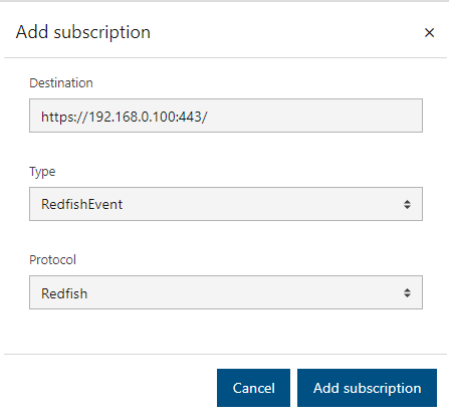
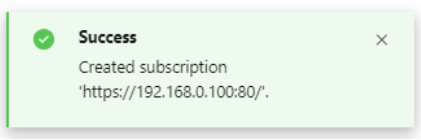
Configuring the Redfish events push to remote listeners

The BMC Redfish Events push can be configured:

- Using the BMC Web UI
- Using Redfish

Configuring the Redfish events push 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, select **Settings** and then **Event Subscriptions** .	
Step_2	Click on the **Add subscription** button.	
Step_3	In the **Add subscription** menu, enter the destination address into the **Destination** field. The destination address should be formatted as follows: **[PROTOCOL]://[ADDRESS]:[PORT]/** **NOTE:** The slash (/) at the end of the destination address is required.	
Step_4	Select **RedfishEvent** from the **Type** dropdown menu.	
Step_5	Select **Redfish** from the **Protocol** dropdown menu.	
Step_6	A success message should appear in the top right corner upon successful configuration.	

Configuring the Redfish events push using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Add a new RedfishEvent subscription

Do so by using this command:
curl -k -s --request POST --url [ROOT_URL]/redfish/v1/EventService/Subscriptions --header 'Content-Type: application/json' --data '{"Destination": "[http or https]://[SERVER IP]:[PORT]", "SubscriptionType": "RedfishEvent", "Protocol": "Redfish"}' | jq
Exemple:

```
$
$ curl -k -s --request POST --url https://admin:ready2go@192.168.8.56/redfish/v1/EventService/Subscriptions --header 'Content-Type: application/json'
--data '{"Destination": "https://192.168.0.111:443/", "SubscriptionType": "RedfishEvent", "Protocol": "Redfish"}' | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "The resource has been created successfully",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Created",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
$
```

Get list of RedfishEvent subscriptions

Do so by using this command:
curl -k -s --request GET --url [ROOT_URL]/redfish/v1/EventService/Subscriptions | jq
Exemple:

```
$ curl -k -s --request GET --url https://admin:ready2go@192.168.8.56/redfish/v1/EventService/Subscriptions | jq
{
  "@odata.id": "/redfish/v1/EventService/Subscriptions",
  "@odata.type": "#EventDestinationCollection.EventDestinationCollection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/EventService/Subscriptions/3466308111"
    }
  ],
  "Members@odata.count": 1,
  "Name": "Event Destination Collections"
}
$
```

Get details about a specific RedfishEvent subscription

Do so by using this command:
curl -k -s --request GET --url [ROOT_URL]/redfish/v1/EventService/Subscriptions/[SubscriptionID] | jq
Exemple:

```
$ curl -k -s --request GET --url https://admin:ready2go@192.168.8.56/redfish/v1/EventService/Subscriptions/3466308111 | jq
{
  "@odata.id": "/redfish/v1/EventService/Subscriptions/3466308111",
  "@odata.type": "#EventDestination.v1_7_0.EventDestination",
  "Context": "",
  "DeliveryRetryPolicy": "TerminateAfterRetries",
  "Destination": "https://192.168.0.111:443/",
  "EventFormatType": "Event",
  "HttpHeaders": [],
  "Id": "3466308111",
  "MessageIds": [],
  "MetricReportDefinitions": [],
  "Name": "Event Destination 3466308111",
  "Protocol": "Redfish",
  "RegistryPrefixes": [],
  "ResourceTypes": [],
  "SubscriptionType": "RedfishEvent",
  "VerifyCertificate": true
}
$
```

Change VerifyCertificate property of a specific subscription

Setting this property to "false" removes a layer of security!
So should be used with extreme precaution!
This property is only relevant for SSL/HTTPS connections.
It provides the option to specify if the BMC https client service will **verify or not the certificate 'authenticity'** of the server prior to sending the events.
Description of this property in the Redfish documentation :
" *Used to verify that the service is communicating with the correct event listener prior to transmitting the event.*"
Could be useful for tests (or in a local secured network) of a Redfish Events Listener tool (ex: GitHub - DMTF/Redfish-Event-Listener) using a certificate self signed or signed by any certificate authority (CA) that BMC can't validate (see footnote 1).
Default value is "true" (certificate authenticity verification done).
Change of this property only affect the specified subscription (all other existant or new ones will keep the "true" default value).
To change the value of the targeted subscription can be done using this command:
curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/EventService/Subscriptions/[subscriptionID] --header 'Content-Type: application/json' --data '{"VerifyCertificate": [true/false]}' | jq
Exemple:

```
$ curl -k -s --request PATCH --url https://admin:ready2go@192.168.8.56/redfish/v1/EventService/Subscriptions/3466308111 --header
'Content-Type: application/json' --data '{"VerifyCertificate": false}' | jq
$
```

Verification of the current/new VerifyCertificate value can be done using the command referred to in the 'Get details about a specific RedfishEvent subscription' section.
[1] Currently, the BMC contains a list of trusted CA certificates used to validate server certificates for its HTTPS client services (got/updated from CA Certs from Mozilla in the firmware build process). Users who want to use certificates signed by authorities not in this list needs to set "VerifyCertificate" to false for SSL/HTTPS connections (until release of a firmware containing what is missing to be able to manually add trusted certificates to the Client Trust Store).

Configuring sensors and thermal parameters

Table of contents

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

	Changes made to thermal parameters will be lost when the BMC is upgraded. However, they are persistent upon rebooting the BMC.

	The information provided in this section is to configure sensors related to the end user PCIe add-in cards. Only the following sensors should be configured by the end user: • Temp PCIe 1 mbox • Temp PCIe 2 mbox • Temp PCIe 1 • Temp PCIe 2 • Temp Chassis

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

There are several methods to configure platform sensors, including:
- Using Redfish
- Using IPMI

	Sensor threshold Upper critical must be bigger than Upper non-critical for the fan controller to properly operate.

Performing configurations using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.
Refer to Creating URLs and Sensor list for sensor information required.

Configuring sensor thresholds

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 -s --request PATCH --url [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 • UpperThresholdCritical • UpperThresholdNonCritical To modify customer-specific PCIe add-in card related sensors, the value for parameter [RESOURCE] is: • Temperatures

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Chassis/ME121
0_Baseboard/Thermal --header 'Content-Type:application/json' --data '{"Temperatures": [{"MemberI
d": "Temp_PCIe_1","UpperThresholdNonCritical": 77}]}' | jq
{
  "@odata.id": "/redfish/v1/Chassis/ME1210_Baseboard/Thermal",
  "@odata.type": "#Thermal.v1_4_0.Thermal",
  "Fans": [],
  "Id": "Thermal",
  "Name": "Thermal",
  "Temperatures": []
}
```

Configuring minimum fan speed

	Minimum fan speed should never be under 30%.

Step_1	Set minimum fan speed. 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_Controller": {"OutLimitMin": [MINIMUM_FAN_SPEED]}}}}}}' | jq
	`$ curl -k -s --request PATCH --url 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`

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.

Step_1	Set maximum fan speed. 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_Controller": {"OutLimitMax": [MAXIMUM_FAN_SPEED]}}}}}}' | jq
	`$ curl -k -s --request PATCH --url 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`

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.

Step_1	Set a threshold offset. RemoteComputer_OSPrompt:~# curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc --header 'Content-Type: application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {" [SENSOR_ID] ": {"ThresholdOffset": [VALUE] }}}}}}' | jq NOTE: The ThresholdOffset value must be negative.
	`$ curl -k -s --request PATCH --url 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`

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 -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc --header 'Content-Type: application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {"[SENSOR_ID]": {"StartPointOffsetFromThreshold": [VALUE]}}}}}}' NOTE: The StartPointOffsetFromThreshold value must be negative.
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header 'Content-Type:application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {"Temp_PCIe_1": {"StartPointOffsetFromThreshold": -9}}}}}}' | jq`

Configuring the minimum ambient temperature

For information on the functionalities linked to the minimum ambient temperature, refer to Platform cooling and thermal management .
The minimum ambient temperature is the Temp Inlet sensor value at which fans will start running at minimum speed. Below this va lue, fans are stopped so the heater can do its work in a cold environment.

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_Controller":{"AmbientTempMin":[VALUE]}}}}}}' | jq
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc --header 'Content-Type:application/json' --data '{"Oem": {"OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"AmbientTempMin": 12}}}}}}' | jq`

Enabling or disabling TelcoAlarm sensor events using Redfish

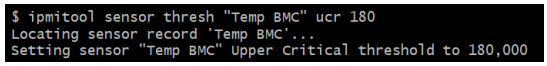
TelcoAlarm sensors are used to monitor the inputs of the alarm connector. If nothing is connected to the alarm connector, TelcoAlarm events will be registered in the SEL every time the BMC reboots. This happens because in order to detect faulty wiring (for example a cut cable) the system considers an open loop as an event—and an empty alarm connector creates an open loop.
If the alarm connector inputs are not used, event generation should be disabled.

Step_1	Enable or disable event generation from TelcoAlarms. RemoteComputer_OSPrompt:~# curl -k [ROOT_URL] /redfish/v1/Managers/bmc -H "Content-Type: application/json" -X PATCH -d '{ "Oem": { "Kontron": {"Discrete": {"TelcoAlarm_Logging":"[STATUS]"}}}}' Possible values for parameter [STATUS] are: • YES – to enable event generation from TelcoAlarms (this is the default value) • NO – to disable event generation from TelcoAlarms
	

Performing configurations using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -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 values for parameter [THRESH_TYPE] are: • unr = upper non-recoverable • ucr = upper critical • unc = upper non-critical • lnc = lower non-critical • lcr = lower critical • lnr = lower non-recoverable	

Configuring the switch

Table of contents

Relevant sections:

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

Changes to the switch NOS configuration are not persistent after rebooting the switch NOS.
To preserve configurations, the current configuration needs to be saved to startup-config.
From the switch NOS Web UI:

- Select **Maintenance** , **Configuration** and then **Save startup-config** . Click on **Save Configuration** to confirm the change.

From the switch NOS 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.

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 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 a ME1310 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	eno1 *	00:89:00.3
Ethernet 1/14	eno2 *	00:89:00.2
Ethernet 1/15	eno3 *	00:89:00.1
Ethernet 1/16	eno4 *	00:89:00.0

* 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	Port 13-16
1	7x SFP+ 10GbE	SFP1-7	4x 10GBASE-KR	Port 13-16
	2x SFP28 25GbE	SFP9-10		
2	2x SFP+ 10GbE	SFP1-2	4x 10GBASE-KR	Port 13-16
	4x SFP28 25GbE	SFP9-12		
3	4x SFP28 25GbE	SFP9-12	4x 25GBASE-KR	Port 13-16
4	10x SFP+ 10GbE	SFP1-9,11	4x 25GBASE-KR	Port 13-16
5	12x SFP+ 10GbE	SFP1-12	2x 25GBASE-KR	Port 13-14
			2x 10GBASE-KR	Port 15-16
6	11x SFP+ 10GbE	SFP1-11	3x 25GBASE-KR	Port 13-15
			1x 10GBASE-KR	Port 16
7	10x SFP+ 10GbE	SFP1-10	2x 25GBASE-KR	Port 13-14
	1x SFP28 25GbE	SFP11	2x 10GBASE-KR	Port 15-16

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 Accessing the switch NOS 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 one currently active:

From EXEC mode

Step_1	Show available port map configuration options and the port map configuration currently active.
	LocalSwitchNOS_OSPrompt:~# **show portmap**
		`# show portmap`
		`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`
		`3   None          1/9-16        1/1-8`
		
		`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 the port map configuration currently active.
	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`
		`--  ------------  ------------  ------------`
		`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`
		`3   None          1/9-16        1/1-8`
		
		`Active port map configuration:    0`

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

```
# show portmap
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
3   None          1/9-16        1/1-8

Active port map configuration:    0
Selected port map configuration:  1
(Selected port map will take effect following switch reboot)
```

Selecting a port map configuration

Step_1	Access the configuration setup menu. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`
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

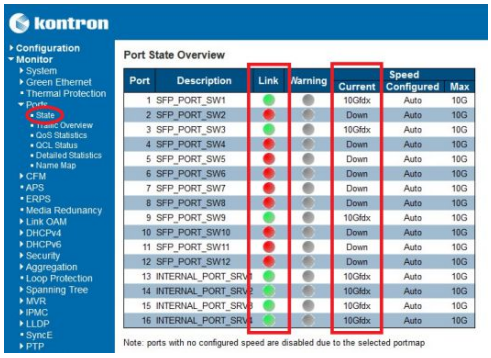
Access the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.

Step_1	Verify every link status. LocalSwitchNOS_OSPrompt:~# **show interface * status**

```
NOS00A0A5E24F56# show interface  * status
Interface  Mode     Speed   Max  Aneg       Media Type SFP Family   Link     Operational Warnings
---------- -------- ------- ---- ---------- ---------- ------------ -------- --------------------
Eth 1/1    Enabled  Auto    10G  No         SFP        10G Optical  10Gfdx
Eth 1/2    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/3    Enabled  Auto    10G  No         SFP        10G Optical  10Gfdx
Eth 1/4    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/5    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/6    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/7    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/8    Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/9    Enabled  Auto    10G  No         SFP        10G DAC      10Gfdx
Eth 1/10   Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/11   Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/12   Enabled  Auto    10G  Unknown    SFP        None         Down
Eth 1/13   Enabled  Auto    10G  Yes (Cl73) SFP        10G CuBP     10Gfdx
Eth 1/14   Enabled  Auto    10G  Yes (Cl73) SFP        10G CuBP     10Gfdx
Eth 1/15   Enabled  Auto    10G  Yes (Cl73) SFP        10G CuBP     10Gfdx
Eth 1/16   Enabled  Auto    10G  Yes (Cl73) SFP        10G CuBP     10Gfdx
```

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 **Monitor** , then **Ports** and then **State**. **NOTE:** This is also the default landing page when accessing the switch NOS Web UI.	

Enabling a switch port

Switch ports can be enabled using:

- The CLI
- The switch Web UI

Enabling a switch port using the CLI

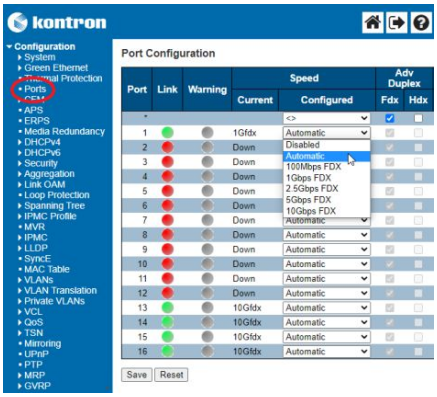
Access the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.
To preserve configurations, the current configuration needs to be saved to startup-config. Refer to Saving the current configuration using the CLI .

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 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 .

Step_1	From the left-side menu, select **Configuration** and then **Ports** .	
Step_2	Enable a switch port by selecting its speed configuration.	
Step_3	Press on the **Save** button to confirm.	
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

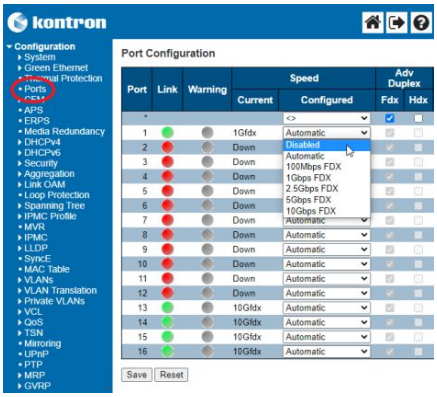
Access the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.
To preserve configurations, the current configuration needs to be saved to startup-config. Refer to Saving the current configuration using the CLI .

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	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 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 .

Step_1	From the left-side menu, select **Configuration** and then **Ports** .	
Step_2	Disable a switch port by changing its speed configuration to **Disabled** .	
Step_3	Press on the **Save** button to confirm.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Changing link speed

Link speed can be changed using:

- The CLI
- The switch Web UI

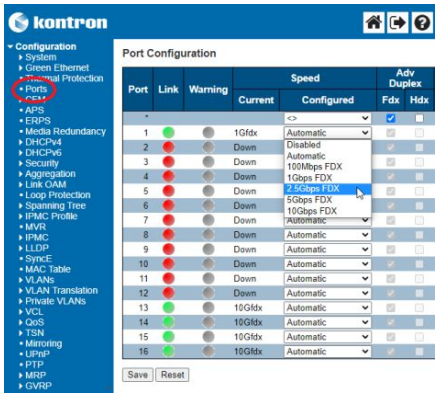
Changing link speed using the CLI

Access the switch NOS CLI. Refer to 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 CLI .

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]**	`(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 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 .

Step_1	From the left-side menu, select **Configuration** , and then **Ports** .	
Step_2	Select a value from the **Speed** dropdown menu.	
Step_3	Press on the **Save** button to confirm.	
Step_4	(Optional) To make the change persistent, save running-config to startup-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

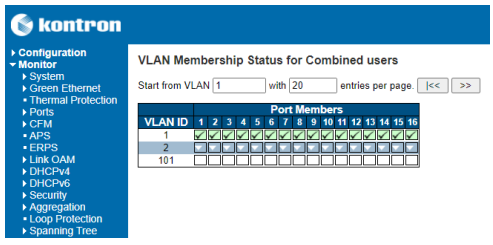
Displaying VLANs using the CLI

Access the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.

Step_1	Display the VLAN status for every switch port.
	LocalSwitchNOS_OSPrompt:~# **show vlan**
		`NOS00A0A5E01C4F# show vlan`
		`VLAN  Name                             Interfaces`
		`----  -------------------------------  ----------`
		`1     default                          Eth 1/1-6`
		`2     VLAN0002                         Eth 1/7`
		`3     VLAN0003                         Eth 1/8-9`

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 **Monitor** , **VLANs** and then **Membership** . The VLAN port membership should be displayed.	

Creating a VLAN

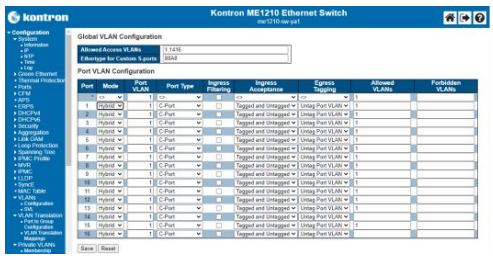
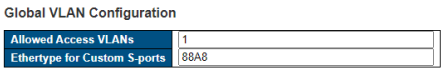
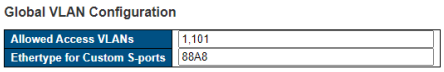
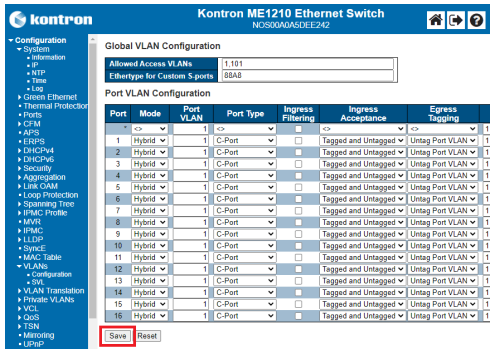
Creating a VLAN using the CLI

Access the switch NOS CLI. 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 CLI .

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 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 .

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-config.	

Removing a VLAN

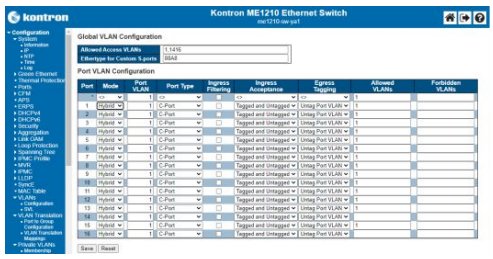
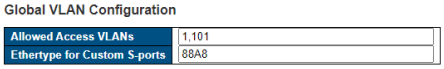
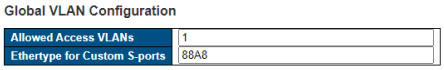
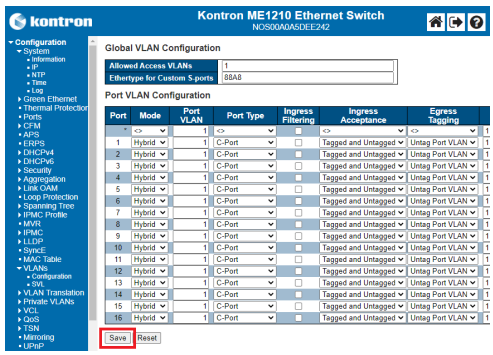
Removing a VLAN using the CLI

Access the switch NOS CLI. 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 CLI .

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 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 .

Step_1	From the left-side menu, navigate to **Configuration** , **VLANs** , and then **Configuration** .	
Step_2	From the **Global VLAN Configuration** , remove the desired VLANs from the **Allowed Access VLANs** list.	 
Step_3	Click on the **Save** button.	
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring VLAN port membership

	The default configuration for the platform 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 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 CLI .

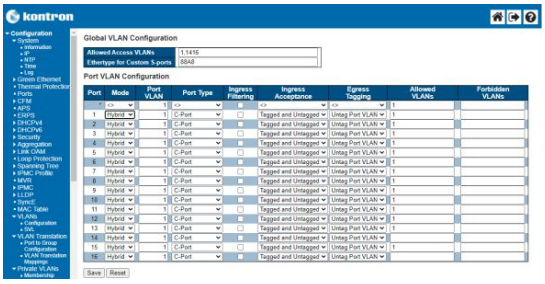
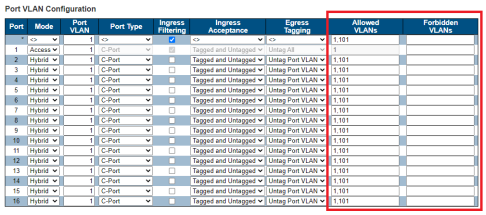
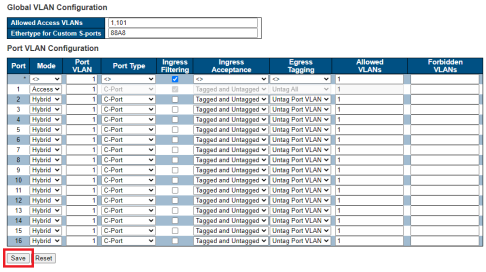
Step_1	Access the desired interface configuration menu. LocalSwitchNOS_OSPrompt:~# **configure terminal** LocalSwitchNOS_OSPrompt:~(config)# **interface [INTERFACE_ID]**	`# configure terminal` `(config)# interface Ethernet 1/3`

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`

Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring port membership using the Web UI

Access the switch NOS 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 .

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	
Step_3	Press on the **Save** button to confirm.	
Step_4	(Optional) To make the change persistent, save running-config to startup-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 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 CLI .

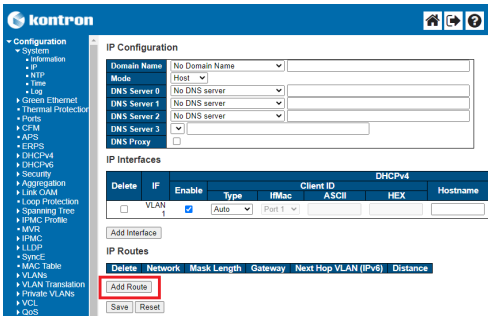
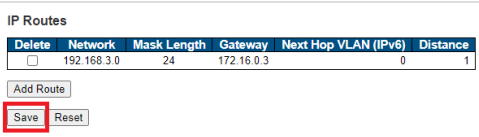
Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`
Step_2	Configure static routing. LocalSwitchNOS_OSPrompt:~(config)# **ip route [HOST_ADDRESS] [NETWORK_MASK] [GATEWAY_ADDRESS]**	`(config)# ip route 192.168.3.0 255.255.255.0 172.16.0.3`
Step_3	Exit 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**
		`# show ip route`
		`Codes: C - connected, S - static`
		`* - FIB route, D - DHCP installed route`
		
		`D* 0.0.0.0/0 [253/0] via 172.16.0.1, VLAN 1, 18:33:31`
		`C* 172.16.0.0/16 is directly connected, VLAN 1, 18:33:31`
		`S* 192.168.3.0/24 [1/0] via 172.16.0.3, VLAN 1, 18:33:31`

Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring static routing using the Web UI

Access the switch NOS 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 .

Step_1	From the left-side menu, select **Configuration** , **System** and then **IP** .	
Step_2	Click on the **Add Route** button.	
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.	
Step_4	Press on the **Save** button to confirm.	
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring a 802.1X authentication pass-through

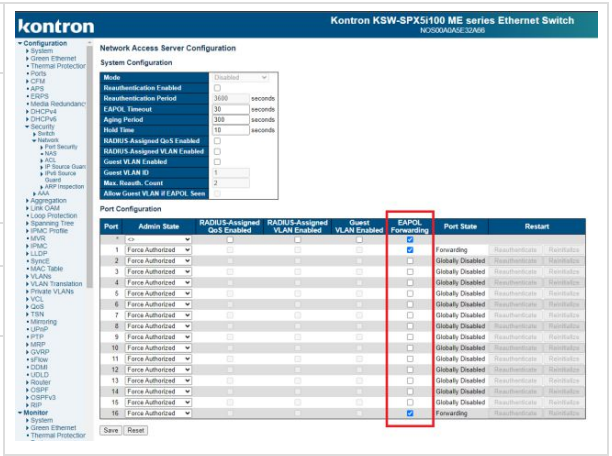
Settings described here configure desired ports to forward specific 802.1X/EAPoL packets. In the case where an 802.1X authentication is desired for an upstream port, since the NOS does not support the Supplicant role, select this option to configure a pass-through of the authentication to a Supplicant running on the integrated Xeon® server. Note that it is not possible to select this option when the authentication system is enabled.

Configuring EAPoL forwarding using the CLI

Step_1	Access the configuration menu. LocalSwitchNOS_OSPrompt:~# **configure terminal**	`# configure terminal`
Step_2	Access the configuration menu of the interface. LocalSwitchNOS_OSPrompt:~# **interface [INTERFACE_ID]**	`# interface Ethernet 1/1`
Step_3	Enable EAPoL forwarding. LocalSwitchNOS_OSPrompt:~# **dot1x eapol-forwarding**	`# dot1x eapol-forwarding`
Step_4	Repeat steps 2 and 3 for all upstream ports requiring authentication and for the integrated server port used by its supplicant application.	
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring EAPoL forwarding using the Web UI

Step_1	From the left-side menu, select **Configuration** , **Security** , **Network** and then **NAS** .
Step_2	Check the **EAPOL Forwarding** column for all upstream ports requiring authentication and for the integrated server port used by its supplicant application. **NOTE:** It is not possible to select this option when the authentication system is enabled.
Step_3	Click on **Save** .
Step_4	(Optional) To make the change persistent, save running-config to startup-config.



Managing the switch configuration

The switch configuration can be managed using:

- The CLI
- The switch Web UI

Managing the switch configuration using the CLI

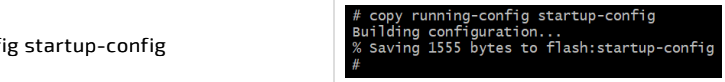
Access the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.

Displaying the running configuration using the CLI

Step_1	Display the current configuration. LocalSwitchNOS_OSPrompt:~# **show running-config**	

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**	

Restoring the default configuration using the CLI

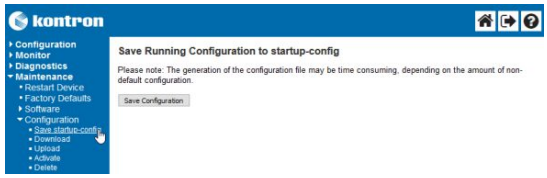
Step_1	Restore the default configuration. LocalSwitchNOS_OSPrompt:~# **reload defaults**	
Step_2	(Optional) To make the change persistent, save running-config to startup-config.	

Managing the switch configuration using the Web UI

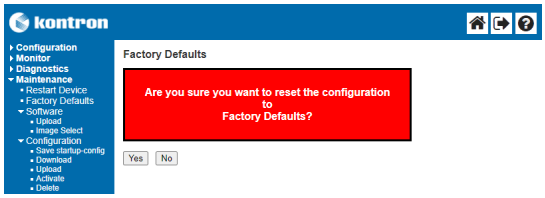
Access the switch NOS Web UI. Refer to Accessing the switch NOS for access instructions.

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 command.

Step_1	From the left-side menu, select **Maintenance** , **Configuration** , and then **Save startup-config** .	
Step_2	Press on the **Save Configuration** button.	

Restoring the default configuration using the Web UI

Step_1	From the left-side menu, select **Maintenance** and then **Factory Defaults** .	
Step_2	Press on the **Yes** button to confirm the choice.	

Configuring synchronization

Table of contents

	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 or slave 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 E823 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

Integrated GNSS receiver

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.

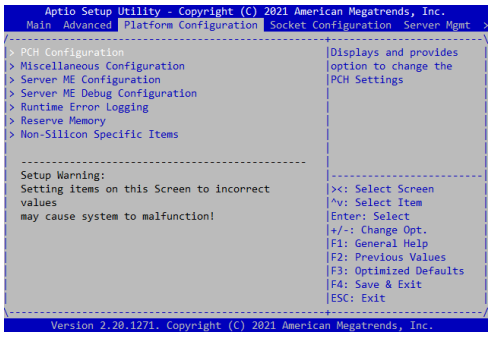
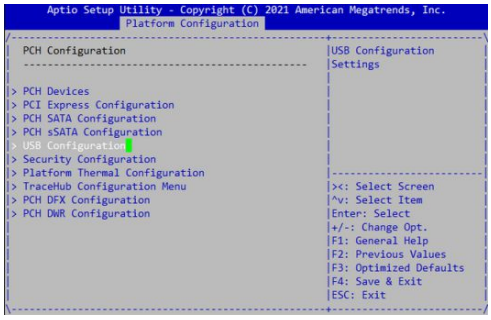
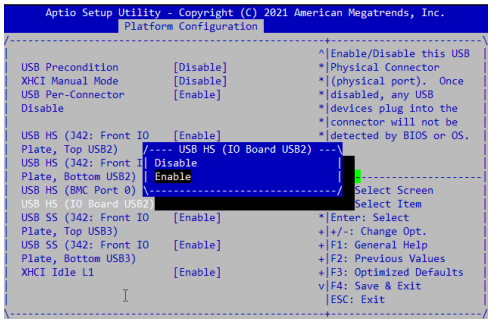
Version 3.22 of the **gpsd** software package is required. Please refer to https://gpsd.gitlab.io/gpsd/index.html for more information.

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.

It is highly recommended to verify the delay compensation using the platform PPS output and/or PTP against a reference from a test equipment on site at installation time.

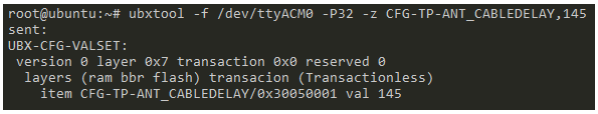
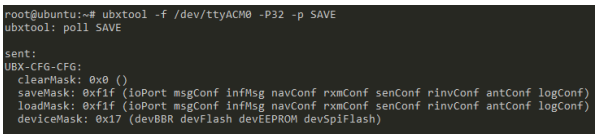
Verifying the status of the USB port connecting the GNSS receiver to the internal server

By default, the USB port connecting the integrated server to the GNSS receiver is disabled.
Log in to the UEFI/BIOS setup menu. Refer to Accessing the UEFI or BIOS for access instructions.

Step_1	From the UEFI/BIOS setup menu, navigate to the **Platform Configuration** tab and select **PCH Configuration** .	
Step_2	Select **USB Configuration** .	
Step_3	Select **USB HS (IO Board USB2)** and ensure its status is set to **Enable** .	

Configuring the antenna delay

Log in to the server. Refer to Accessing the operating system of a server 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]**	
Step_2	Save the configuration to flash. Server_OSPrompt:~# **ubxtool -f /dev/ttyACM0 -P32 -p SAVE**	

i	With the default configuration, the GNSS receiver is automatically available to be used by the Ethernet switch NOS. The GNSS receiver becomes the timing synchronization source when a PTP instance 0 is configured for master only mode. It can also be enabled as a synchronization source in boundary clock mode. This is described below.
i	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 1/13 to 1/16 and use LinuxPTP to synchronize time with the integrated server's E823 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

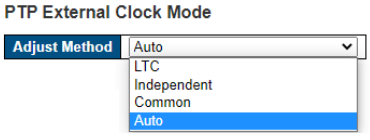
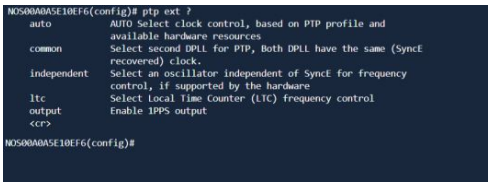
Relevant section:
SMA PPS output

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

The only configurable parameter is the clock adjustment method. Default setting **Auto** is equivalent to "Common" for IEEE1588 and G.8275.1 profiles. The methods available are:

- **Common** : The PTP clock uses the hardware DPLL for PTP frequency adjustment with the SyncE frequency as a reference if available. Available for clock instance 0 only.
- **Independent** : T he PTP clock uses the hardware DPLL for PTP frequency adjustment with only the local oscillator for frequency reference. This would only be for a deployment where the SyncE reference is not considered valid for the PTP clock instance. Available for clock instance 0 only.
- **LTC (Local Time Counter)** : The PTP clock instance uses the Ethernet switch local time counter for frequency adjustment. This is the only option for clock instances 1 to 3 since the hardware DPLL is bound to clock instance 0. Note that this also implies that if clock instance 0 is synchronized to a master, the LTCs for clock instances 1 to 3 will have their frequencies determined by that master.

NOS Web UI	NOS CLI
	

Creating a switch NOS PTP instance

i	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 examples show 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.

Relevant section:
SMA GNSS RF input pinout and electrical characteristics

Configuring the switch as a telecom grandmaster using the CLI

Log in to the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.

Step_1	Enter configuration mode. LocalSwitchNOS_Prompt# **configure terminal**	`NOS00A0A5E10EF6# configure terminal` `NOS00A0A5E10EF6(config)#`
Step_2	Create the PTP clock instance "0". Then add the desired interface(s) to "ptp 0", the clock instance created. LocalSwitchNOS_Prompt(config)# **ptp 0 mode master profile g8275.1** **NOTE** : Changing the default **filter-type** is not supported in this configuration.	`NOS00A0A5E10EF6(config)# ptp 0 mode master profile g8275.1`

Step_3	The following items configure the PTP dataset communicated by the instance. The values here are valid when the instance has achieved PHASE_LOCKED state.
	LocalSwitchNOS_Prompt(config)# **ptp 0 virtual-port time-property utc-offset 37 valid time-traceable freq-traceable ptptimescale time-source 32**
	ptp 0 virtual-port class 6
	ptp 0 virtual-port accuracy 33
	ptp 0 virtual-port variance 20061
	NOTE : The **utc-offset** value changes in time and should be chosen according to the current value.
		`NOS00A0A5E10EF6(config)# $req-traceable ptptimescale time-source 32`
		`NOS00A0A5E10EF6(config)# ptp 0 virtual-port class 6`
		`NOS00A0A5E10EF6(config)# ptp 0 virtual-port accuracy 33`
		`NOS00A0A5E10EF6(config)# ptp 0 virtual-port variance 20061`

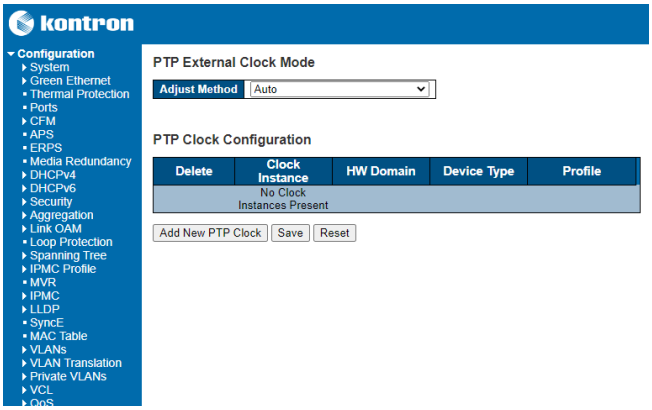
Step_4	(Optional) Set the NOS system time from the PTP instance. LocalSwitchNOS_Prompt(config)# **ptp system-time set** **NOTE:** NTP needs to be disabled in order to set the NOS system time from the PTP instance. Disable it with the command **no ntp** .	`NOS00A0A5E10EF6(config)# ptp system-time set` `System clock synch mode (Set System time from PTP time)`
Step_5	Add interfaces to the PTP instance. LocalSwitchNOS_Prompt(config)# **interface Ethernet 1/1,9,12** LocalSwitchNOS_Prompt(config-if)# **ptp 0**	`NOS00A0A5E10EF6(config)# interface Ethernet 1/1,9,12` `NOS00A0A5E10EF6(config-if)# ptp 0`
Step_6	End configuration. LocalSwitchNOS_OSPrompt(config-if)# **end**	`NOS00A0A5E10EF6(config-if)# end` `NOS00A0A5E10EF6#`

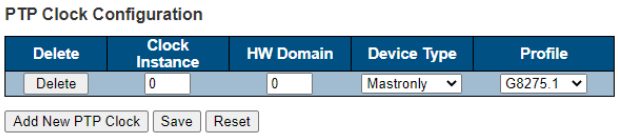
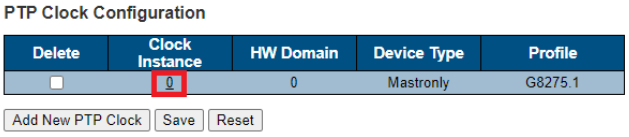
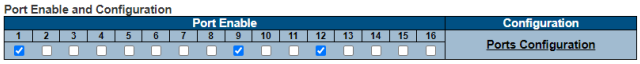
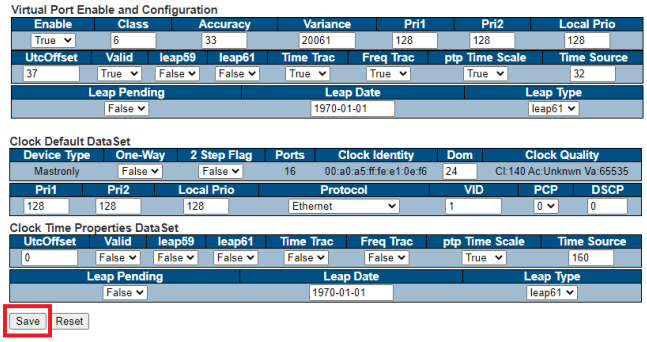
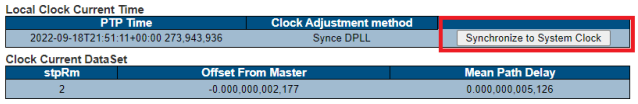
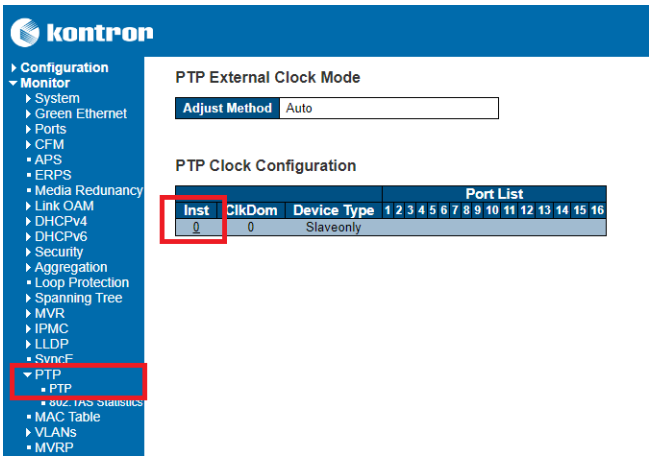
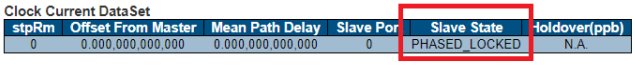
Step_7	Verify the current ptp 0 status.
	LocalSwitchNOS_OSPrompt# **show ptp 0**
	NOTE: The desired "Slave state" status to be attained is **PHASE_LOCKED** . Interim steps that can be displayed are **FREQ_LOCKING** , **FREQ_LOCKED** and **HOLDOVER** . The time to reach **PHASE_LOCKED** varies depending on many factors including the status of the GNSS receiver. Five minutes is typical.
		`NOS00A0A5E10EF6# show ptp 0`
		`Dynamic data for PTP Clock Instance 0:`
		
		`PTP Time: 2022-06-29T16:25:43+00:00 902,081,031`
		
		`Clock Slave state:`
		`Slave Port: 0`
		`Slave State: PHASED_LOCKED`
		`Filter Mode: PACKET`
		`Holdover (ppb): N.A.`
		
		`Clock Current DataSet:`
		`Steps Removed: 0`
		`Offset From Master: 0.000,000,000,000`
		`Mean Path Delay: 0.000,000,000,000`

Step_8	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the switch as a telecom grandmaster using the Web UI

Log in to the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.

Step_1	From the left-side menu, select **Configuration** and then **PTP** .	

		
Step_2	From the **PTP Clock Configuration** section, configure the **Clock Instance** . Then, set the **Device Type** to **Mastronly** and the **Profile** to G8275.1. Finally, click on the **Save** button.	
Step_3	Click on the **Clock Instance** number in order to access the **PTP Clock's Configuration and Status** . **NOTE** : Changing the default **filter-type** is not supported in this configuration.	
Step_4	From the **Port Enable and Configuration** section, select the ports on which to enable PTP.	
Step_5	From the **Virtual Port Enable and Configuration** section, configure the PTP Clock instance using the following values: • Enable: True • Class: 6 • Accuracy: 33 • Variance: 20061 • UtcOffset: 37 • Valid: True • Time Trac: True • Freq Trac: True • ptp Time Scale: True • Time Source: 32 Ensure that the VID matches one of the allowed VLANs for the selected port(s).	
Step_6	Click on the **Save** button.	
Step_7	Set the system time source to PTP by clicking on **Synchronize to System Clock**.	
Step_8	From the left-side menu, select **Monitor**, then **PTP** and then **PTP** again . Click on the instance number of the desired PTP clock.	
Step_9	From the **Clock Current DataSet** section, ensure that the **Slave State** is in the desired state. **NOTE:** The desired "Slave state" status to be attained is **PHASE_LOCKED** . Interim steps that can be displayed are **FREQ_LOCKING** , **FREQ_LOCKED** and **HOLDOVER** . The time to reach **PHASE_LOCKED** varies depending on many factors. As a reference, less than 5 minutes is typical.	
Step_10	(Optional) To make the change persistent, save running-config to 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 virtual port can be enabled for the telecom boundary clock as for the grand master configuration. In this case, it participates in the BMCA as any other PTP foreign masters.

Prerequisite

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

Configuring the switch as a telecom boundary clock using the CLI

Log in to the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.

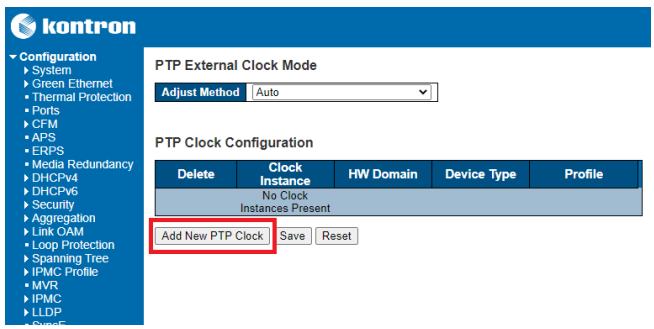
Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt# **configure terminal**	`NOS00A0A5E10EF6# configure terminal` `NOS00A0A5E10EF6(config)#`
Step_2	Create the PTP clock instance "0". Then add the desired interface(s) to "ptp 0", the clock instance created. LocalSwitchNOS_OSPrompt(config)# **ptp 0 mode boundary profile g8275.1** **NOTE** : Changing the default **filter-type** is not supported in this configuration.	`NOS00A0A5E10EF6(config)# ptp 0 mode boundary profile g8275.1`
Step_3	(Optional) Set the NOS system time from the PTP instance. LocalSwitchNOS_OSPrompt(config)# **ptp system-time set** **NOTE:** NTP needs to be disabled in order to set the NOS system time from the PTP instance. Disable it with the command **no ntp** .	`NOS00A0A5E10EF6(config)# ptp system-time set` `System clock synch mode (Set System time from PTP time)`
Step_4	Add interfaces to the PTP instance. This includes interfaces connected to the potential network T-GM as well as interfaces connected to downstream slave clocks (T-BC or T-SL). Ports will assume master or slave mode automatically. LocalSwitchNOS_OSPrompt(config)# **interface Ethernet 1/1,9,12** LocalSwitchNOS_OSPrompt(config-if)# **ptp 0**	`NOS00A0A5E10EF6(config)# interface Ethernet 1/1,9,12` `NOS00A0A5E10EF6(config-if)# ptp 0`
Step_5	End configuration. LocalSwitchNOS_OSPrompt(config-if)# **end**	`NOS00A0A5E10EF6(config-if)# end` `NOS00A0A5E10EF6#`

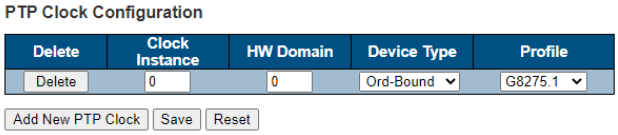
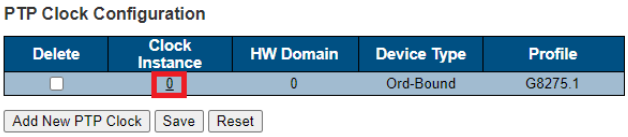
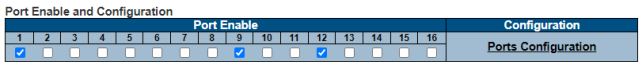
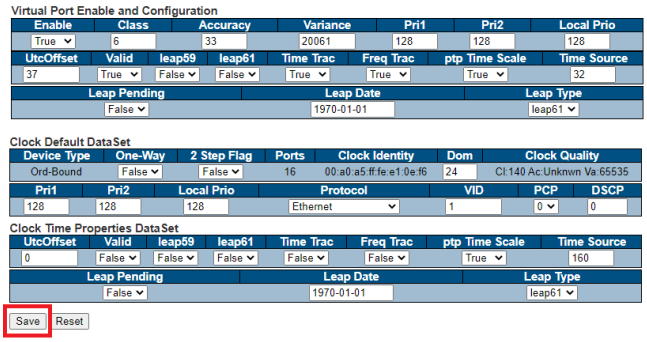
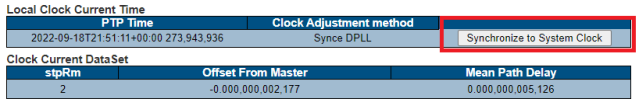
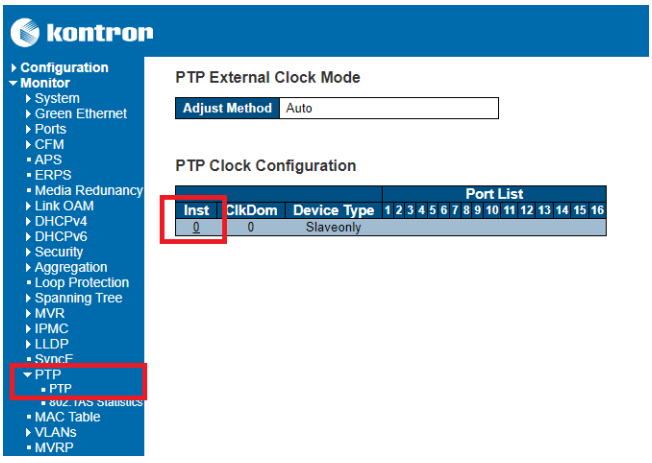
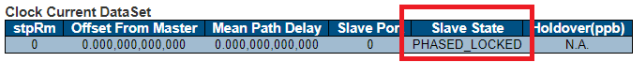
Step_6	Verify the current ptp 0 status.
	LocalSwitchNOS_OSPrompt# **show ptp 0**
	NOTE: The desired "Slave state" status to be attained is **PHASE_LOCKED** . Interim steps that can be displayed are **FREQ_LOCKING** , **FREQ_LOCKED** and **HOLDOVER** . The time to reach **PHASE_LOCKED** varies depending on many factors. As a reference, less than 5 minutes is typical.
		`NOS00A0A5E10EF6# show ptp 0`
		`Dynamic data for PTP Clock Instance 0:`
		
		`PTP Time: 2022-06-29T16:25:43+00:00 902,081,031`
		
		`Clock Slave state:`
		`Slave Port: 0`
		`Slave State: PHASED_LOCKED`
		`Filter Mode: PACKET`
		`Holdover (ppb): N.A.`
		
		`Clock Current DataSet:`
		`Steps Removed: 0`
		`Offset From Master: 0.000,000,000,000`
		`Mean Path Delay: 0.000,000,000,000`

Step_7	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the switch as a telecom boundary clock using the Web UI

Log in to 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 **PTP** . Click, on the **Add New PTP Clock** button.	

		
Step_2	From the **PTP Clock Configuration** section, configure the **Clock Instance** . Then, set the **Device Type** to **Ord-Bound** and the **Profile** to **G8275.1**. Finally, click on the **Save** button.	
Step_3	Click on the **Clock Instance** number in order to navigate to the **PTP Clock's Configuration and Status** .	
Step_4	From the **Port Enable and Configuration** section, select the ports on which to enable PTP. This includes interfaces connected to the potential network T-GM as well as interfaces connected to downstream slave clocks (T-BC or T-SL). Ports will assume master or slave mode automatically.	
Step_5	From the **Virtual Port Enable and Configuration** section, configure the PTP Clock instance. Ensure that the VID matches one of the allowed VLANs for the selected port(s).	
Step_6	Click on the **Save** button.	
Step_7	Set the system time source to PTP by clicking on **Synchronize to System Clock.**	
Step_8	From the left-side menu, select **Monitor**, then **PTP** and then **PTP** again . Click on the instance number of the desired PTP clock.	
Step_9	From the **Clock Current DataSet** section, ensure that the **Slave State** is in the desired state. **NOTE:** The desired "Slave state" status to be attained is **PHASE_LOCKED** . Interim steps that can be displayed are **FREQ_LOCKING** , **FREQ_LOCKED** and **HOLDOVER** . The time to reach **PHASE_LOCKED** varies depending on many factors. As a reference, less than 5 minutes is typical.	
Step_10	(Optional) To make the change persistent, save running-config to startup-config.	

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.

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

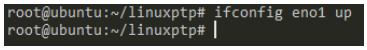
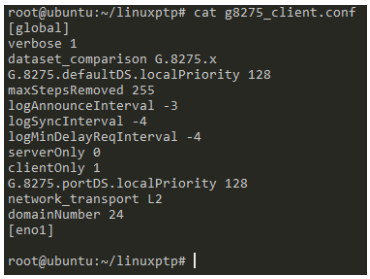
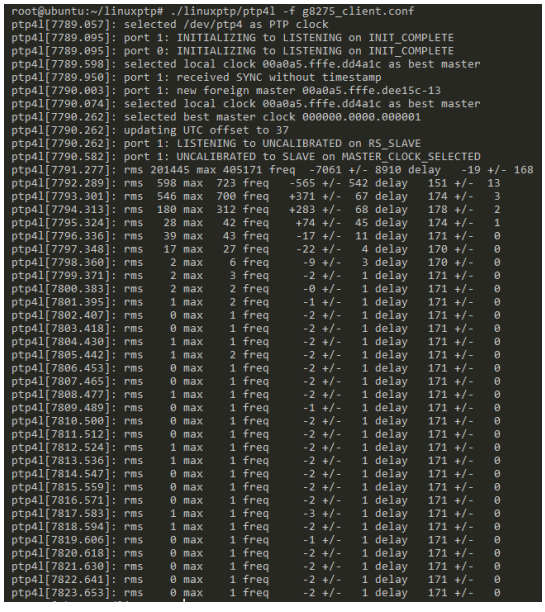
Synchronizing the E823 PTP hardware clock

Prerequisite

1	The switch must be configured as a T-GM or a T-BC as explained above. In the example below, interface 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.
2	The latest driver for the E823-C Ethernet controller is installed.

Procedure

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

Step_1	Make sure the network interface is up. Server_OSPrompt:~# **ifconfig eno1 up**	
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]**	
Step_3	Run ptp4l. Server_OSPrompt:~# **./linuxptp/ptp4l -f g8275_client.conf**	

Synchronizing the integrated server system time

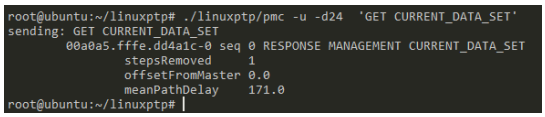
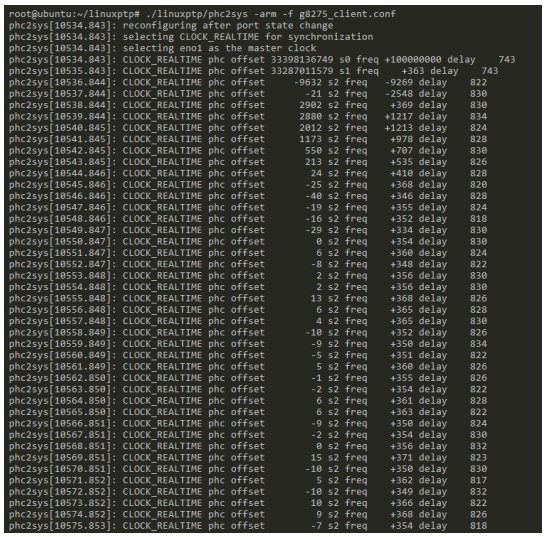
Prerequisite

1	A **ptp4l** instance running on the platform's operating system is required prior to this test.

	Make sure there is no time synchronization daemon (NTP or other) running since it will interfere.

Procedure

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

Step_1	Verify the running ptp4l status. Server_OSPrompt:~# **./linuxptp/pmc -u -d24 'GET CURRENT_DATA_SET'**	
Step_2	Synchronize the physical hardware clock (PHC) with the system clock. Server_OSPrompt:~# **./linuxptp/phc2sys -arm -f g8275_client.conf**	

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.
	Synchronization of the integrated server's switch ports (interfaces 1/13-1/16) is not relevant since the platform clocking architecture achieves this automatically.

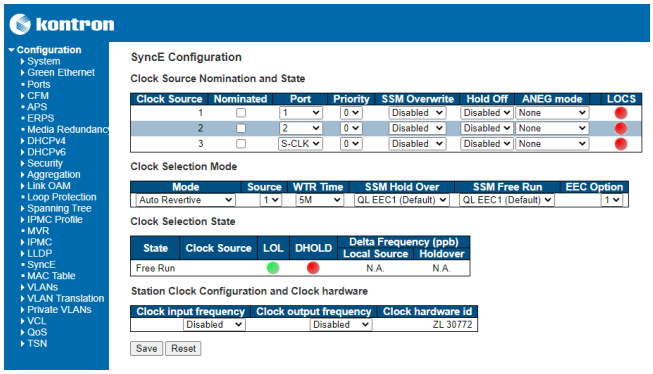
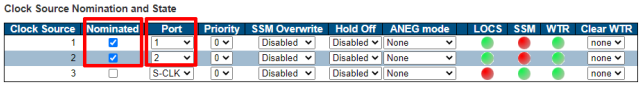
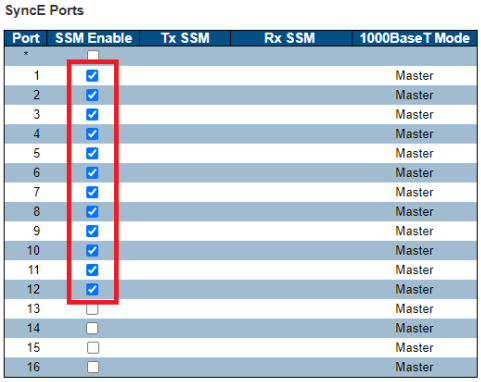
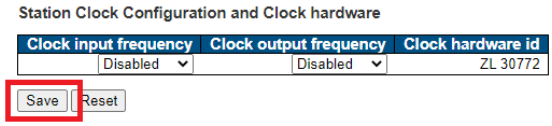
Configuring synchronous Ethernet using the CLI

Log in to the switch NOS CLI. Refer to Accessing the switch NOS for access instructions.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt# **configure terminal**	NOS00A0A5DEE15C# configure terminal NOS00A0A5DEE15C(config)#
Step_2	Nominate interfaces where clock synchronization sources will be connected. Up to two sources can be configured. **NOTE:** Clock source number 3 is locked to the station clock which is not used in this platform. SSM can be enabled on: • Clock source interfaces where the source will be sending status messages. Note that source interfaces will not be used by the switch unless the appropriate SSM messages are received. • Interfaces where the platform integrated switch will be a SyncE source to link partners expecting SSM messages to enable their synchronization. In the example: • Interfaces 1/1 and 1/2 are connected to SyncE sources sending SSM status information. So they are nominated and configured for SSM to monitor the sources. • Interfaces 1/3-1/12 configured for SSM can be used by link partners requiring a SyncE source and expecting SSM status information. LocalSwitchNOS_OSPrompt(config)# **network-clock clk-source 1 nominate interface Ethernet 1/1** LocalSwitchNOS_OSPrompt(config)# **network-clock clk-source 2 nominate interface Ethernet 1/2** LocalSwitchNOS_OSPrompt(config)# **interface Ethernet 1/1-12** LocalSwitchNOS_OSPrompt(config-if)# **network-clock synchronization ssm**	NOS00A0A5DEE15C(config)# net$clk-source 1 nominate interface Ethernet 1/1 NOS00A0A5DEE15C(config)# net$ock clk-source 2 nominate interface Ethernet 1/2 NOS00A0A5DEE15C(config)# interface Ethernet 1/1-12 NOS00A0A5DEE15C(config-if)# network-clock synchronization ssm NOS00A0A5DEE15C(config-if)#
Step_3	End configuration. LocalSwitchNOS_OSPrompt(config-if)# **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 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 1/5 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 NOS00A0A5DEE15C#
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring synchronous Ethernet using the Web UI

Log in to 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 **SyncE** .	
Step_2	From the **Clock Source Nomination and State** section, nominate and select the interface number (general nomenclature 1/x where x is the targeted selection here) where clock synchronization sources will be connected. Up to two sources can be configured. **NOTE:** Clock source number 3 is locked to the station clock which is not used in this platform. In the example, interfaces 1/1 and 1/2 are connected to SyncE sources, so are configured to clock sources 1 and 2.	
Step_3	From the **SyncE Ports** section, SSM can be enabled on: • Clock source interfaces where the source will be sending status messages. Note that source interfaces will not be used by the switch unless the appropriate SSM messages are received. • Interfaces where the platform integrated switch will be a SyncE source to link partners expecting SSM messages to enable their synchronization. In the example: • Interfaces 1/1 and 1/2 are connected to SyncE sources sending SSM status information. So they are configured for SSM to monitor the sources. • Interfaces 1/3-1/12 can be used by link partners requiring a SyncE source and expecting SSM status information.	
Step_4	Click on the **Save** button.	
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring UEFI/BIOS options

Table of contents

Relevant section:
Platform power management

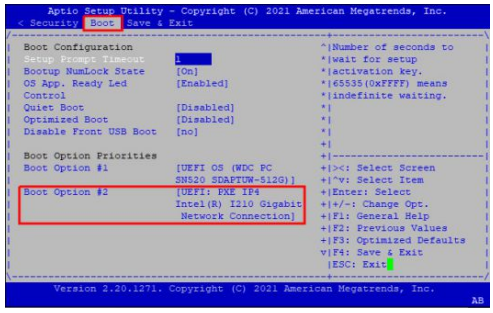
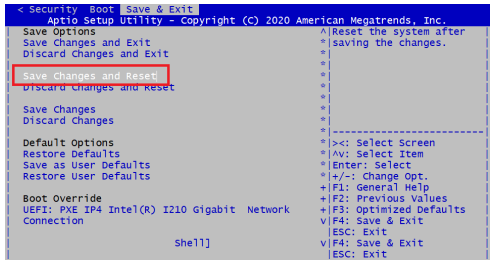
Options can be configured:

- Using the UEFI/BIOS menu
- Via the BMC using Redfish

Configuring UEFI/BIOS options via the UEFI/BIOS menu

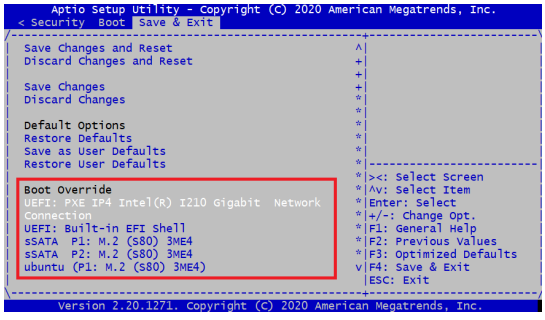
Access the UEFI/BIOS. Refer to Accessing the UEFI or BIOS for access instructions.

Changing the boot order

Step_1	From the UEFI/BIOS setup menu, navigate to the **Boot** menu. Configure the boot order as desired.	
Step_2	Select the **Save & Exit** menu, go to **Save Changes and Reset** and press **Enter** to confirm and save the new boot order.	

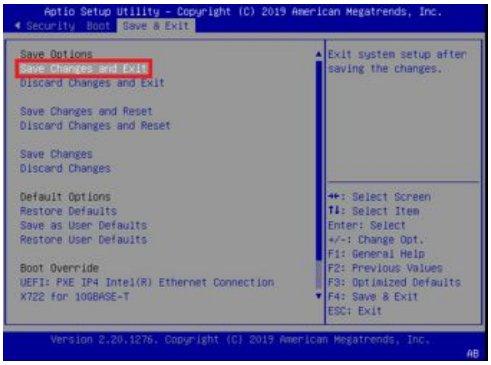
Overriding the boot order

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

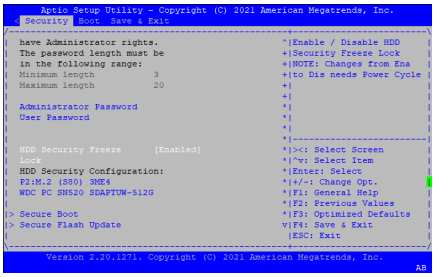
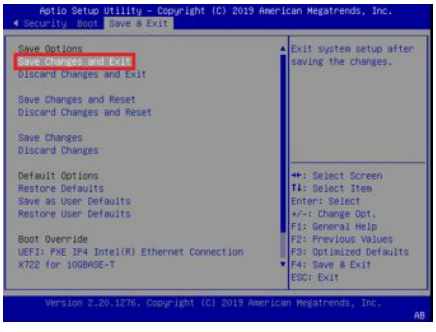
Step_1	Reboot the platform and access the UEFI/BIOS setup menu.	
Step_2	Navigate to the **Save & Exit** menu and then to the **Boot Override** section.	

Enabling Secure Boot

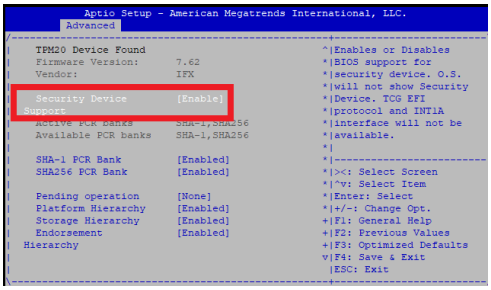
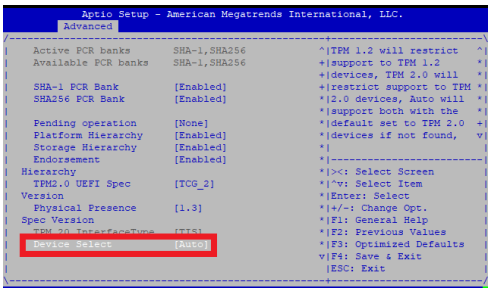
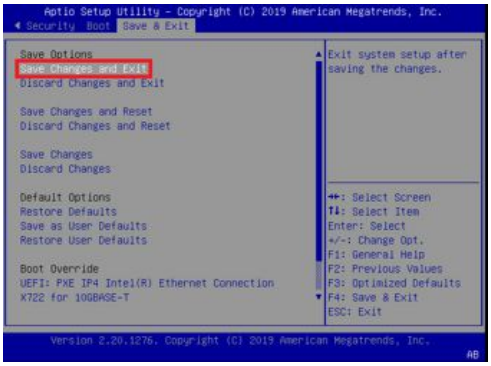
The following application notes are required to generate secure boot keys and configure them: Generating custom secure boot keys and Provisioning custom secure boot keys.

Step_1	Navigate to the **Security** tab and access the **Secure Boot** submenu.	
Step_2	Select the **Secure Boot** option and change it to **Enabled** .	
Step_3	Use the application notes mentioned above as reference to generate and configure secure boot keys.	
Step_4	Navigate to the **Save & Exit** menu, go to **Save Changes and Exit** and press **Enter** to confirm.	

Performing an HDD Security Freeze Lock

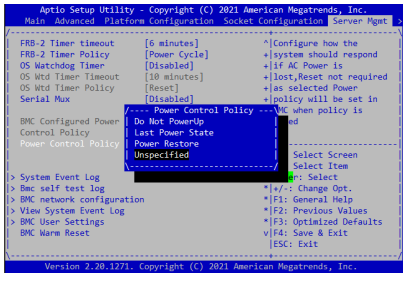
Step_1	Navigate to the **Security** tab, and enable or disable the **HDD Security Freeze Lock** .	
Step_2	Navigate to the **Save & Exit** menu, go to **Save Changes and Exit** and press **Enter** to confirm.	

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: [Enable / Disable] **NOTE:** The TPM has to be inserted to see the menu.	
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 / TCG_2] **NOTE:** The TPM has to be inserted to see the menu.	
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 / Auto] **NOTE:** The TPM has to be inserted to see the menu.	
Step_4	Navigate to the **Save & Exit** menu, go to **Save Changes and Exit** and press **Enter** to confirm.	

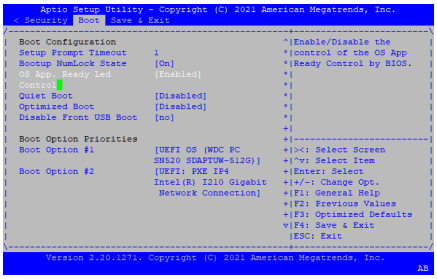
Configuring the server Power Control Policy

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

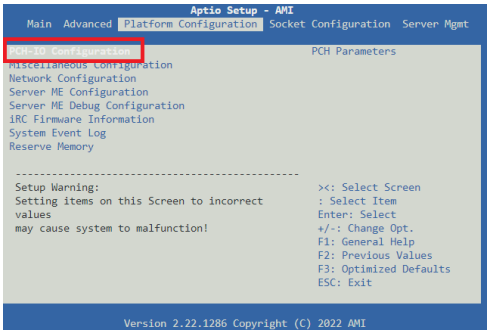
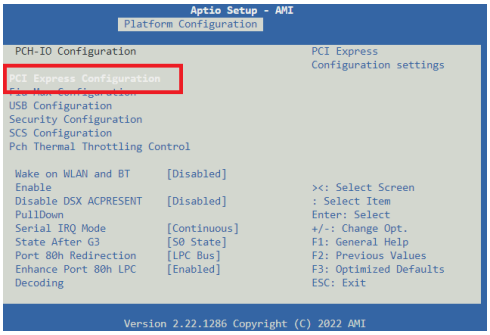
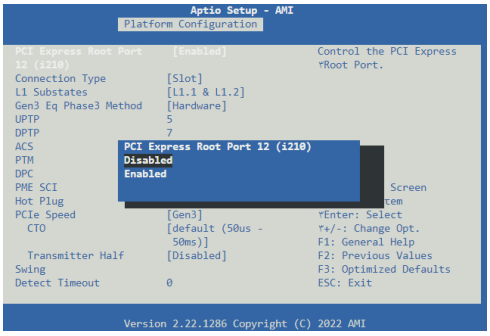
Step_1	Navigate to the **Server Mgmt** menu. Select **Power Control Policy** and choose the option according to the response desired. Possible values: [Do Not PowerUp / Last Power State / Power Restore / Unspecified] **NOTE:** This configuration is saved in the BMC and does not require a server reset. **NOTE:** Selecting Do Not PowerUp or Last Power State means that a command must be sent to the BMC to power up and boot the integrated server as there is no power button on the unit.	

Configuring option Application Ready LED

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

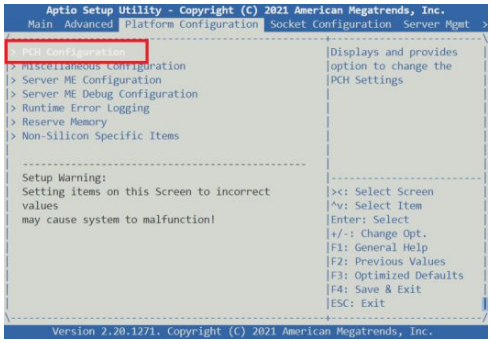
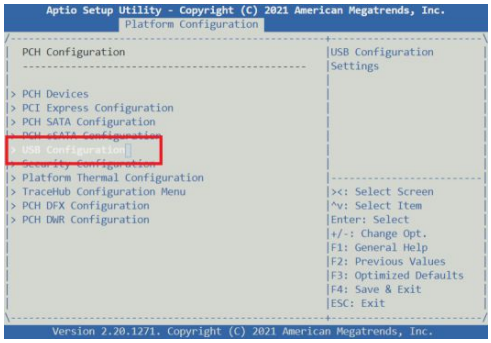
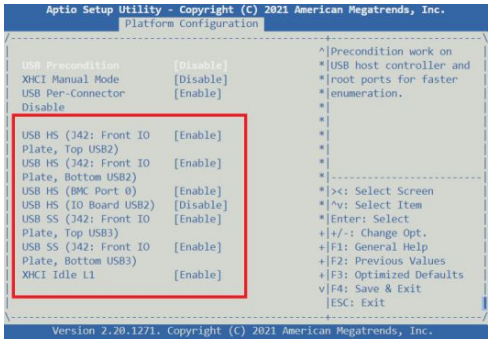
Step_1	Navigate to the **Boot** menu, and enable or disable the **OS App. Ready Led Control** given to the UEFI/BIOS.	

Disabling server access to the I210 Ethernet controller

Step_1	Navigate to the **Platform Configuration** tab and select **PCH-IO Configuration** .	
Step_2	Navigate to **PCI Express Configuration** .	
Step_3	Navigate to device **PCI Express Root Port 12 (i210)** and select **Disabled** . This will effectively disconnect the I210 Ethernet controller from the server.	

Disabling USB ports

NOTE: Enabling or disabling platform USB ports may cause the system to malfunction. Proceed with caution.

Step_1	Navigate to the **Platform Configuration** tab and select **PCH-IO Configuration** or **PCH Configuration** depending on the UEFI/BIOS firmware version.	
Step_2	Select **USB Configuration** .	
Step_3	All USB ports are identified in this menu. Enable or disable ports as needed according to the following considerations: 1. It is not recommended to change the USB port configuration except for the ports described below. Otherwise, it may leave the platform inoperable. 2. Front panel USB ports are labeled as **Front IO Plate.** Support for USB 3.0 and USB 2.0 must be enabled/disabled separately. 3. Do not disable **BMC Port 0** unless you wish to disable Redfish functionality for the UEFI/BIOS firmware. This would also disable the front-panel MGMTUSB port.	

Configuring UEFI/BIOS options via the BMC using Redfish

This option will be available in a future platform software release.

Specifying the next boot device via the BMC using Redfish

Step_1	Get a list of available boot devices. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system | jq .Boot**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system
 | jq .Boot
{
    "AutomaticRetryAttempts": 3,
    "AutomaticRetryConfig": "RetryAttempts",
    "AutomaticRetryConfig@Redfish.AllowableValues": [
        "Disabled",
        "RetryAttempts"
    ],
    "BootSourceOverrideEnabled": "Continuous",
    "BootSourceOverrideTarget": "BiosSetup",
    "BootSourceOverrideTarget@Redfish.AllowableValues": [
        "None",
        "Pxe",
        "Hdd",
        "Cd",
        "Diags",
        "BiosSetup",
        "Usb"
    ],
    "TrustedModuleRequiredToBoot": "Disabled"
}
```

Step_2	Change the next boot device. The **OVERRIDE_TYPE** value can take one of the following values: • Continuous • Once • None RemoteComputer_OSPrompt:~# **curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Systems/system --header 'Content-Type: application/json' --data '{ "Boot": { "BootSourceOverrideTarget": "[BOOT_DEVICE]", "BootSourceOverrideEnabled": " [OVERRIDE_TYPE] " } }' | jq**

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems
/system --header 'Content-Type:application/json' --data '{"Boot": {"BootSourceOverrideTarg
et": "Hdd","BootSourceOverrideEnabled": "Continuous"}}' | jq
```

Operating

Platform power management

Table of contents

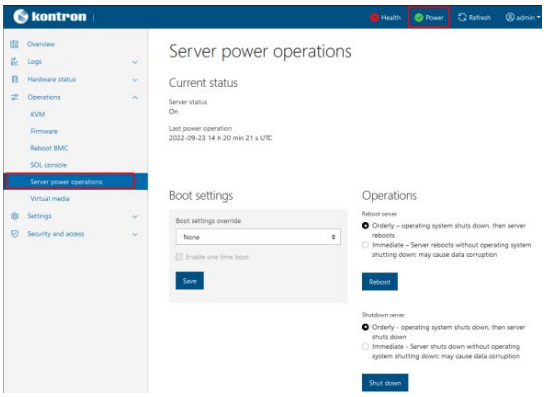
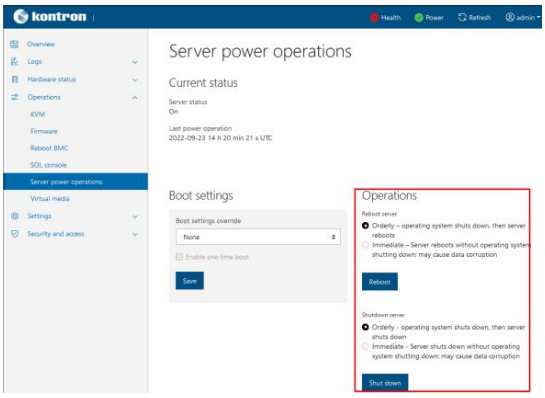
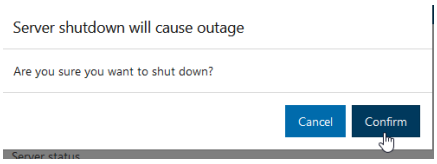
Integrated server power management

A power action command can be executed using:

- The BMC Web UI
- Redfish
- IPMI over LAN

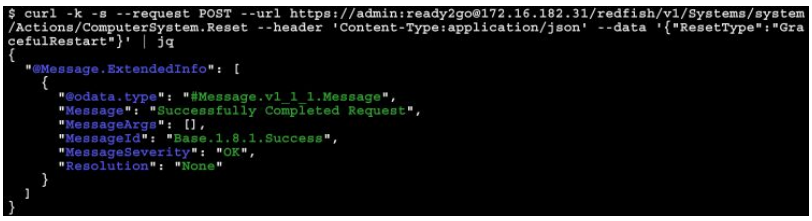
Integrated server power management using the BMC Web UI

Refer to Accessing a BMC using the Web UI for access instructions.
NOTE: Performing a server power action using the Web UI will make the user exit the current window.

Step_1	From the left-side menu, click on **Operations** and then **Server power operations** or simply click on the **Power** status icon at the top of the page.	
Step_2	Click on the desired power action button.	
Step_3	Click the **Confirm** button to continue. The platform will perform the power action.	

Integrated server power management using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Execute the following command to manage platform power. RemoteComputer_OSPrompt:~$ curl -k -s --request POST --url [ROOT_URL]/redfish/v1/Systems/system/Actions/ComputerSystem.Reset --header 'Content-Type: application/json' - -data '{"ResetType":"[POWER_ACTION]"}' | jq Supported values for parameter [POWER_ACTION] are: • On • ForceOff • ForceOn • ForceRestart • GracefulRestart • GracefulShutdown • PowerCycle
	
Step_2	Verify the current power state. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system | jq .PowerState
	

Integrated server power management using IPMI over LAN (IOL)

Refer to Accessing a BMC using IPMI over LAN (IOL) for access instructions.
Power actions can be executed from the integrated server operating system using IPMI via KCS.
NOTE: Performing a power off from the integrated server will make it inaccessible. A power on command would need to be executed using another BMC access method.

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	
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]	
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	

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.

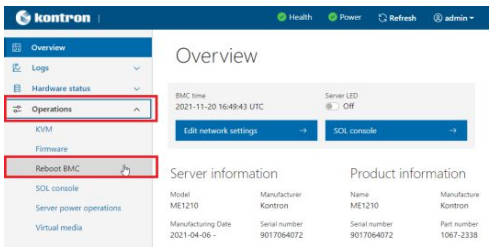
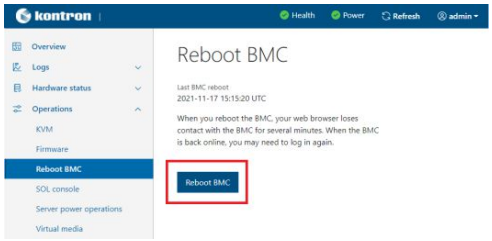
Rebooting the BMC

A BMC reboot can be executed using:
- the BMC Web UI
- Redfish

Rebooting the BMC using the Web UI

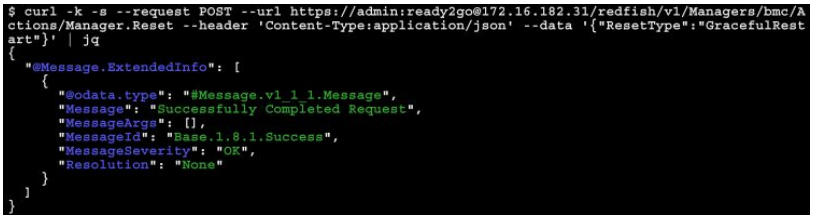
Refer to Accessing a BMC using the Web UI for access instructions.

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

Step_1	From the left-side menu, click on **Operations** and then **Reboot BMC** .	
Step_2	Click on the **Reboot BMC** button and then confirm.	
Step_3	Wait for the BMC to boot. It may take a moment.	

Rebooting the BMC using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Execute the following command to reboot BMC. RemoteComputer_OSPrompt:~$ **curl -k -s --request POST --url [ROOT_URL] /redfish/v1/ Managers /bmc/Actions/Manager.Reset --header 'Content-Type: application/json' --data '{"ResetType":"GracefulRestart"}' | jq** 
Step_2	Wait for the BMC to reboot. It may take a moment.

Rebooting the switch NOS

A switch NOS reboot can be executed using:

- the switch NOS CLI
- the switch NOS Web UI

Rebooting the switch NOS using the NOS CLI

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 Configuring the switch .

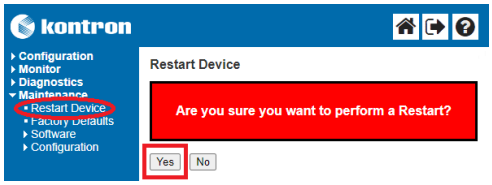
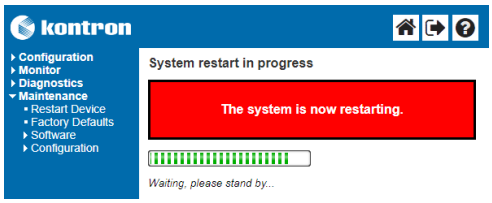
Refer to Accessing the switch NOS for access instructions.

Step_1	LocalSwitchNOS_OSPrompt:~# **reload cold** **NOTE:** Rebooting the switch NOS may take several seconds.

Rebooting the switch NOS using the NOS Web UI

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 Configuring the switch .

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

Step_1	From the left-side menu, select **Maintenance** and then **Restart Device** .	
Step_2	Click on the **Yes** button to begin the restart procedure.	
Step_3	Wait for the switch to be available again. **NOTE:** Rebooting the switch NOS may take several seconds.	

BMC session management

Table of contents

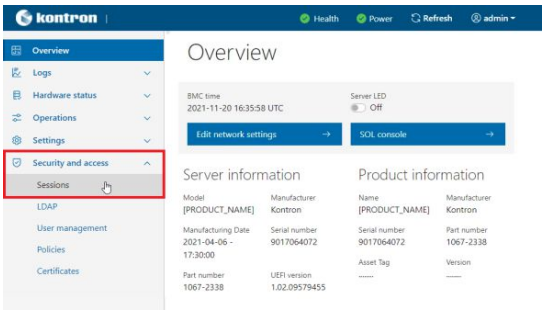
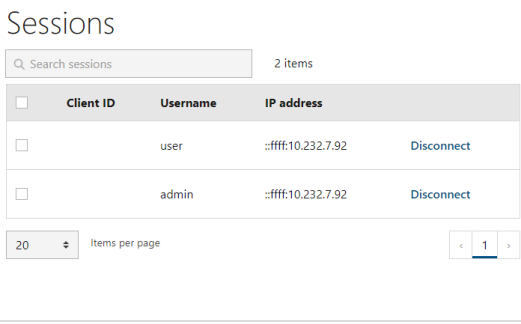
Viewing BMC sessions

BMC sessions can be accessed:

- Using the BMC Web UI
- Using Redfish

Viewing BMC sessions 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 **Security and access** and then **Sessions** .	
Step_2	The session list should be displayed.	

Viewing BMC sessions using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Display the list of active sessions using the following command. Note the session URL. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/SessionService/Sessions | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/SessionService/
Sessions | jq
{
  "@odata.id": "/redfish/v1/SessionService/Sessions/",
  "@odata.type": "#SessionCollection.SessionCollection",
  "Description": "Session Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/SessionService/Sessions/TzsDHTSiJk"
    },
    {
      "@odata.id": "/redfish/v1/SessionService/Sessions/ppt1YBKbx7"
    }
  ],
  "Members@odata.count": 2,
  "Name": "Session Collection"
}
```

Step_2	Access the information on a specific session using the following command. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/SessionService/Sessions/[SESSION_URL] | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/SessionService/
Sessions/TzsDHTSiJk | jq
{
  "@odata.id": "/redfish/v1/SessionService/Sessions/TzsDHTSiJk",
  "@odata.type": "#Session.v1_3_0.Session",
  "ClientOriginIPAddress": "::ffff:10.232.7.92",
  "Description": "Manager User Session",
  "Id": "TzsDHTSiJk",
  "Name": "User Session",
  "UserName": "user"
}
```

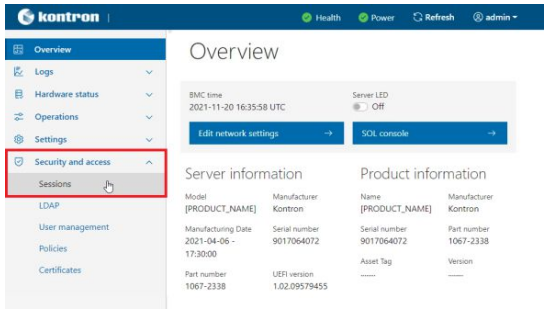
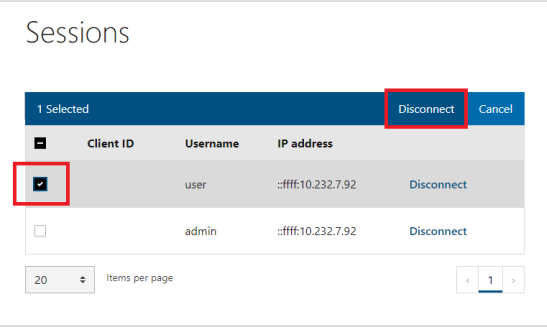
Disconnecting BMC sessions

BMC sessions can be accessed:

- Using the BMC Web UI
- Using Redfish

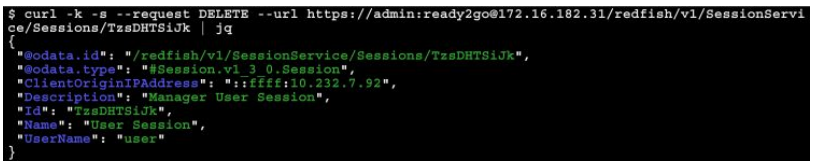
Disconnecting BMC sessions using the BMC Web UI

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 **Security and access** and then **Sessions** .	
Step_2	Select the session(s) to disconnect using the checkboxes and then click on **Disconnect** . **NOTE:** This procedure could end the current BMC session.	

Disconnecting a BMC session using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

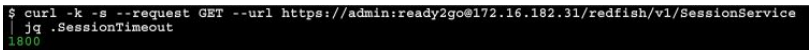
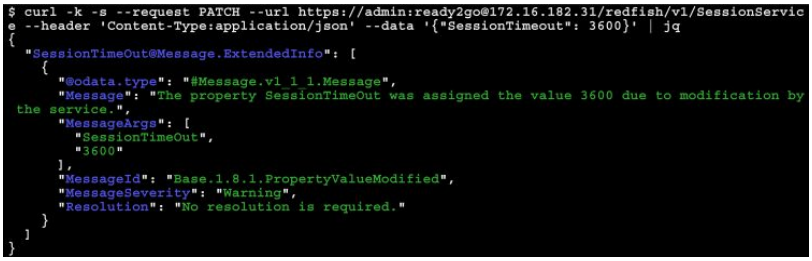
Step_1	Display the list of active sessions using the following command. Note the session URL of the session to disconnect. RemoteComputer_OSPrompt:~# curl -k -s --request GET --url [ROOT_URL]/redfish/v1/SessionService/Sessions | jq
	
Step_2	Delete the session using the following command. RemoteComputer_OSPrompt:~# curl -k -s --request DELETE --url [ROOT_URL]/redfish/v1/SessionService/Sessions/[SESSION_URL] | jq
	

Configuring BMC session timeout

A BMC session will automatically be disconnected after the session timeout expires. This value can be changed if needed.
The default BMC session timeout is 1800 seconds.
The BMC session timeout can only be configured using Redfish.

Configuring BMC session timeout using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Display the current BMC session timeout value. RemoteComputer_OSPrompt:~# curl -k -s --request GET --url [ROOT_URL] /redfish/v1/SessionService | jq .SessionTimeout
	
Step_2	Change the current BMC session timeout to the new desired value. RemoteComputer_OSPrompt:~# curl -k -s --request PATCH --url [ROOT_URL] /redfish/v1/SessionService --header 'Content-Type:application/json' --data '{"SessionTimeout": [TIMEOUT]}'| jq
	

Redfish token-based authentication

This section describes how an HTTPS client can obtain an authentication token through the Redfish API. Throughout the user documentation, basic authentication is used in order to simplify documentation. However, hard-coding user names and passwords can become a security impediment. In order to improve platform security, token-based authentication can be used.
Token-based Redfish authentication can also reduce BMC response time.

Prerequisites

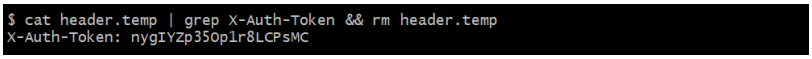
1	The BMC IP address is known.
2	An HTTP client tool is installed on the remote computer.

Creating a session token

Relevant section:
Default user names and passwords

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.

Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Request a session token from the session service. The **Id** of the newly created session should be displayed. RemoteComputer_OSPrompt:~$ **curl -k -s --insecure --request POST --url https:// [BMC MNGMT_IP] /redfish/v1/SessionService/Sessions --header 'Content-Type: application/json' --data '{"UserName": "[BMC_USERNAME]", "Password": "[BMC_PASSWORD]"}' --dump-header [FILE_NAME] | jq**
	
Step_2	Extract the token from the response header from the temporary file and delete it. RemoteComputer_OSPrompt:~$ **cat [FILE_NAME] | grep X-Auth-Token && rm [FILE_NAME]**
	
Step_3	Verify that the token is valid by accessing a Redfish resource. Add the token as an additional header. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url https:// [BMC MNGMT_IP] /redfish/v1/UpdateService --header 'X-Auth-Token: [TOKEN] ' | jq**
	

System inventory

Table of contents

Here is the information that can be collected to create a system inventory:

- FRU information
- BMC, UEFI, FPGA firmware versions
- Power supply type
- Product IO module information
- Processor device information
- Memory device configuration
- UEFI/BIOS configuration
- Ethernet switch running configuration
- Ethernet switch version

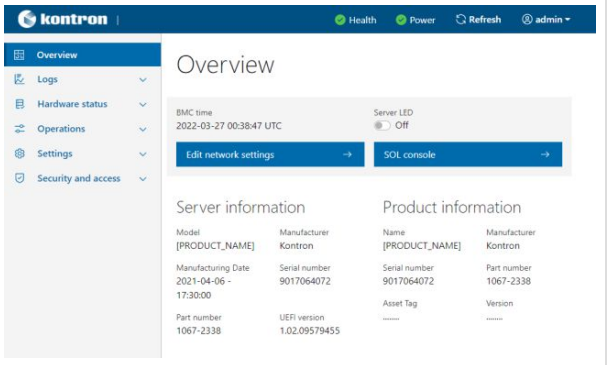
Collecting the FRU information

FRU information can be collected:

- Using the BMC Web UI
- Using Redfish
- Using IPMI

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.

Step_1	From the left-side menu of the BMC Web UI, select **Overview** . The FRU information should be displayed.	

Collecting the FRU information using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Use the following command to collect the FRU information. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system | jq ".Manufacturer, .ManufactureDate, .Model, .PartNumber, .ProductManufacturer, .ProductName, .ProductPartNumber, .ProductSerialNumber"**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system
| jq ".Manufacturer, .ManufactureDate, .Model, .PartNumber, .ProductManufacturer, .ProductName,
.ProductPartNumber, .ProductSerialNumber"

"Kontron"
"2021-04-06 - 17:30:00"
"ME1310"
"1067-2338"
"Kontron"
"ME1310"
"1067-2338"
"9017064072"
```

Collecting the FRU information using IPMI

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

Step_1	Use the following command to collect the FRU information. LocalServer_OSPrompt:~# **ipmitool fru print** **NOTE:** This command will return all detected FRU devices including PCIe add-on cards with FRU EEPROM.	

```
# ipmitool fru print
FRU Device Description : Builtin FRU Device (ID 0)
 Chassis Type          : Main Server Chassis
 Chassis Part Number   : XXXX-XXXX
 Chassis Serial        : XXXXXXXXXX
 Chassis Extra         : ME1310
 Board Mfg Date        : Wed Apr  7 13:30:00 2021
 Board Mfg             : Kontron
 Board Product         : ME1310
 Board Serial          : 9017064072
 Board Part Number     : 1067-2338
 Board Extra           : MAC=00:A0:A5:E1:0E:20/07
 Product Manufacturer  : Kontron
 Product Name          : ME1310
 Product Part Number   : 1067-2338
 Product Version       : ........
 Product Serial        : 9017064072
 Product Asset Tag     : ........

FRU Device Description : ME1310-PSU-DC (ID 74)
 Board Mfg Date        : Mon Jun  1 04:00:00 2020
 Board Mfg             : Kontron
 Board Product         : ME1310-PSU-DC
 Board Serial          : 9017067765
 Board Part Number     : 1067-4309

FRU Device Description : ME1310-SW-X (ID 212)
 Board Mfg Date        : Mon Aug 12 11:55:00 2019
 Board Mfg             : Kontron
 Board Product         : ME1310-SW-X
 Board Serial          : XXXXXXXXXX
 Board Part Number     : .........
 Board Extra           : MAC=CC:CC:CC:CC:CC:CC/DD
```

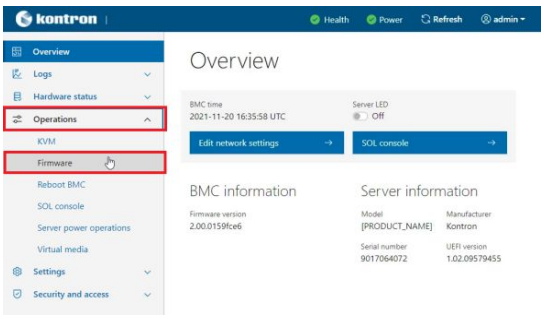
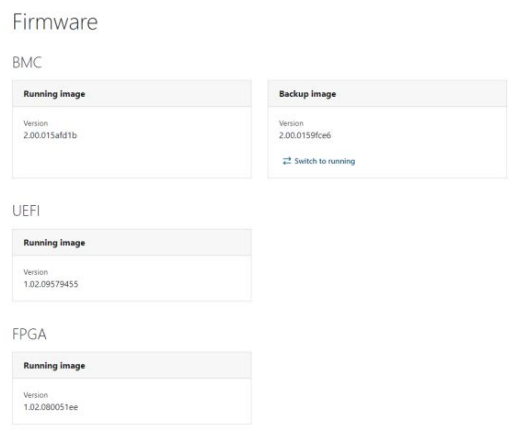
Collecting the BMC, UEFI and FPGA firmware versions

The BMC, UEFI and FPGA firmware versions can be collected:

- Using the BMC Web UI
- Using Redfish

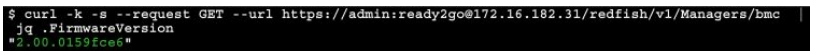
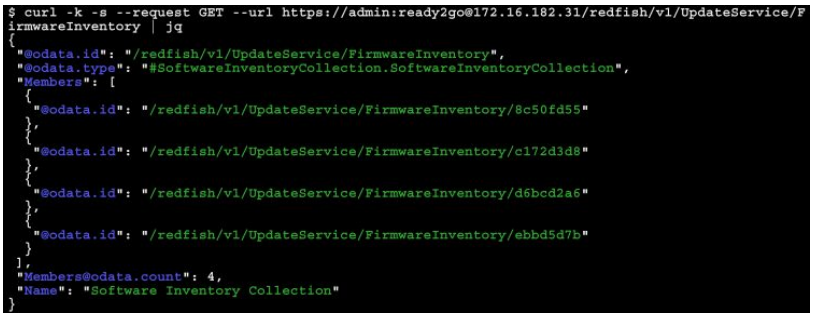
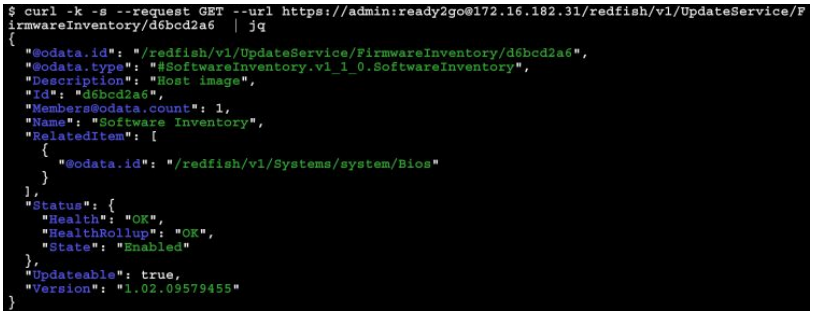
Collecting the BMC, UEFI and FPGA firmware versions using the BMC Web UI

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 **Operations** and then **Firmware** .	
Step_2	The BMC, UEFI/BIOS and FPGA firmware versions will be displayed.	

Collecting the BMC, UEFI and FPGA firmware versions using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Collect the current BMC firmware version using the following command. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc | jq .FirmwareVersion
	
Step_2	Compile the firmware in the BMC Redfish Firmware Inventory. The URLs given by the command below will be used in Step_3. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL] /redfish/v1/UpdateService/FirmwareInventory | jq
	
Step_3	For each URL in the list generated at Step_2, run this command to obtain more information about the firmware images. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL] /redfish/v1/ [URL_FROM_STEP_2] | jq
	

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
- Processor device information
- Memory device configuration

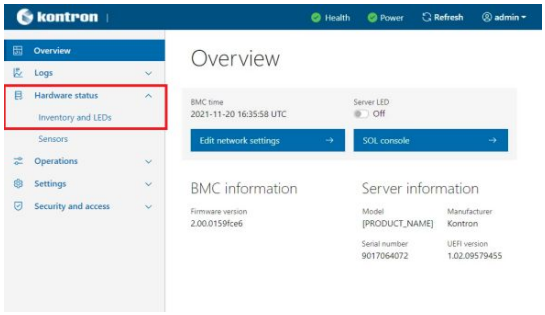
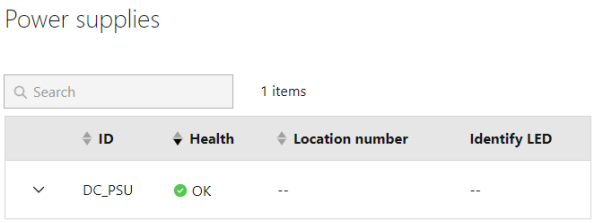
Collecting power supply type (AC or DC)

The power supply type can be collected:

- Using the BMC Web UI
- Using Redfish
- Using IPMI

Collecting power supply type using t he 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** .	
Step_2	From the **Power supplies** section, collect the power supply type.	

Collecting power supply type using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Collect the power supply type using the following command. The power supply type can either be DC or AC. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Chassis/ME1310_Baseboard/Power | jq .PowerSupplies**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Chassis/M
E1310_Baseboard/Power | jq .PowerSupplies
[
  {
    "@odata.id": "/redfish/v1/Chassis/ME1310_Baseboard/Power#/PowerSupplies/0",
    "EfficiencyPercent": 90,
    "Manufacturer": "Kontron",
    "MemberId": "MERS_DC_PSU",
    "Model": "ME1310-PSU-DC",
    "Name": "MERS DC PSU",
    "PartNumber": "1067-4309",
    "PowerOutputWatts": 62,
    "SerialNumber": "9017067765",
    "Status": {
      "Health": "OK",
      "State": "Enabled"
    }
  }
]
```

Collecting power supply type using IPMI

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

Step_1	Use the following command to collect the FRU information. The power supply should appear in the devices listed by the command. LocalServer_OSPrompt:~# **ipmitool fru print** **Power supply types:** AC PSU: M1877 DC PSU: ME1310-PSU-DC	

```
# ipmitool fru print
FRU Device Description : Builtin FRU Device (ID 0)
 Chassis Type          : Main Server Chassis
 Chassis Part Number   : XXXX-XXXX
 Chassis Serial        : XXXXXXXXXX
 Chassis Extra         : ME1310
 Board Mfg Date        : Wed Apr  7 13:30:00 2021
 Board Mfg             : Kontron
 Board Product         : ME1310
 Board Serial          : 9017064072
 Board Part Number     : 1067-2338
 Board Extra           : MAC=00:A0:A5:E1:0E:20/07
 Product Manufacturer  : Kontron
 Product Name          : ME1310
 Product Part Number   : 1067-2338
 Product Version       : ........
 Product Serial        : 9017064072
 Product Asset Tag     : ........

FRU Device Description : ME1310-PSU-DC (ID 74)
 Board Mfg Date        : Mon Jun  1 04:00:00 2020
 Board Mfg             : Kontron
 Board Product         : ME1310-PSU-DC
 Board Serial          : 9017067765
 Board Part Number     : 1067-4309

FRU Device Description : ME1310-SW-X (ID 212)
 Board Mfg Date        : Mon Aug 12 11:55:00 2019
 Board Mfg             : Kontron
 Board Product         : ME1310-SW-X
 Board Serial          : XXXXXXXXXX
 Board Part Number     : ........
 Board Extra           : MAC=CC:CC:CC:CC:CC:CC/DD
```

Collecting product IO module information

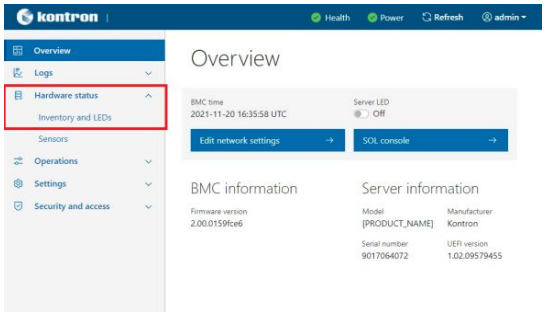
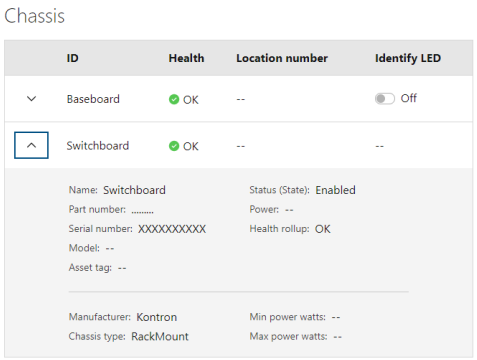
The product IO module information can be collected:

- Using the BMC Web UI

- Using Redfish
- Using IPMI

Collecting product IO module i nformation using t he 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** .	
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.	

Collecting product IO module i nformation using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Identify the type of IO module using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Chassis | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Chassis |
 jq
{
 "@odata.id": "/redfish/v1/Chassis",
 "@odata.type": "#ChassisCollection.ChassisCollection",
 "Members": [
  {
   "@odata.id": "/redfish/v1/Chassis/ME1310_Baseboard"
  },
  {
   "@odata.id": "/redfish/v1/Chassis/Switchboard"
  }
 ],
 "Members@odata.count": 2,
 "Name": "Chassis Collection"
}
```

Step_2	Collect the IO module information using the following command and the URL obtained at the previous step. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Chassis/[IO_MODULE_URL] | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Chassis/S
witchboard  | jq
{
  "@odata.id": "/redfish/v1/Chassis/Switchboard",
  "@odata.type": "#Chassis.v1_14_0.Chassis",
  "Actions": {
    "#Chassis.Reset": {
      "@Redfish.ActionInfo": "/redfish/v1/Chassis/Switchboard/ResetActionInfo",
      "target": "/redfish/v1/Chassis/Switchboard/Actions/Chassis.Reset"
    }
  },
  "ChassisType": "RackMount",
  "Id": "Switchboard",
  "Links": {
    "ComputerSystems": [
      {
        "@odata.id": "/redfish/v1/Systems/system"
      }
    ],
    "ManagedBy": [
      {
        "@odata.id": "/redfish/v1/Managers/bmc"
      }
    ]
  },
  "Manufacturer": "Kontron",
  "Model": "ME1310-SW-X",
  "Name": "Switchboard",
[...]
```

Collecting product IO module i nformation using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To

use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17** .

Step_1	Use the following command to collect the FRU information. LocalServer_OSPrompt:~# **ipmitool fru print** **IO module type:** Switchboard = ME1310-SW-X IOBoard = ME1310-IOS	

```
# ipmitool fru print
FRU Device Description : Builtin FRU Device (ID 0)
 Chassis Type          : Main Server Chassis
 Chassis Part Number   : XXXX-XXXX
 Chassis Serial        : XXXXXXXXXX
 Chassis Extra         : ME1310
 Board Mfg Date        : Wed Apr  7 13:30:00 2021
 Board Mfg             : Kontron
 Board Product         : ME1310
 Board Serial          : 9017064072
 Board Part Number     : 1067-2338
 Board Extra           : MAC=00:A0:A5:E1:0E:20/07
 Product Manufacturer  : Kontron
 Product Name          : ME1310
 Product Part Number   : 1067-2338
 Product Version       : ........
 Product Serial        : 9017064072
 Product Asset Tag     : ........

FRU Device Description : ME1310-PSU-DC (ID 74)
 Board Mfg Date        : Mon Jun  1 04:00:00 2020
 Board Mfg             : Kontron
 Board Product         : ME1310-PSU-DC
 Board Serial          : 9017067765
 Board Part Number     : 1067-4309

FRU Device Description : ME1310-SW-X (ID 212)
 Board Mfg Date        : Mon Aug 12 11:55:00 2019
 Board Mfg             : Kontron
 Board Product         : ME1310-SW-X
 Board Serial          : XXXXXXXXXX
 Board Part Number     : .........
 Board Extra           : MAC=CC:CC:CC:CC:CC:CC/DD
```

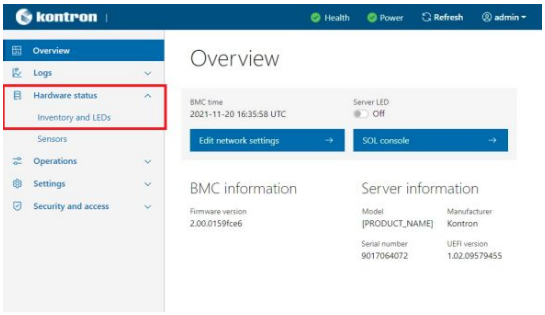
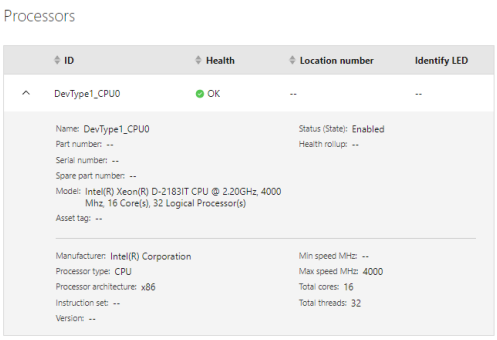
Collecting processor device information

The processor device information can be collected:

- Using the BMC Web UI
- Using Redfish

Collecting processor device information 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** .	
Step_2	From the **Processors** section, collect the processor configuration information.	

Collecting processor device information using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	List all the processor devices using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Systems/system/Processors | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/
Processors | jq
{
 "@odata.id": "/redfish/v1/Systems/system/Processors",
 "@odata.type": "#ProcessorCollection.ProcessorCollection",
 "Members": [
  {
   "@odata.id": "/redfish/v1/Systems/system/Processors/DevType1_CPU0"
  }
 ],
 "Members@odata.count": 1,
 "Name": "Processor Collection"
}
```

Step_2	Collect processor device information using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Systems/system/Processors/[DEVICE_URL] | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/
Processors/DevType1_CPU0 | jq
{
 "@odata.context": "/redfish/v1/$metadata#Processor.Processor",
 "@odata.id": "/redfish/v1/Systems/system/Processors/DevType1_CPU0",
 "@odata.type": "#Processor.v1_1_0.Processor",
 "CurrentFrequency": 2200,
 "Id": "DevType1_CPU0",
 "Manufacturer": "Intel(R) Corporation",
 "MaxSpeedMHz": 4000,
 "Model": "Intel(R) Xeon(R) D-2183IT CPU @ 2.20GHz, 4000 Mhz, 16 Core(s), 32 Logical Processor(s
)",
 "Name": "DevType1_CPU0",
 "ProcessorArchitecture": "x86",
 "ProcessorId": {
  "EffectiveFamily": "Intel(R) Xeon(R) D-2183IT CPU @ 2.20GHz"
 },
 "ProcessorType": "CPU",
 "Socket": "CPU0",
 "Status": {
  "Health": "OK",
  "State": "Enabled"
 },
[...]
```

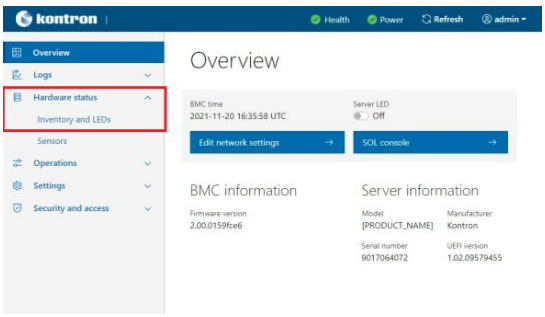
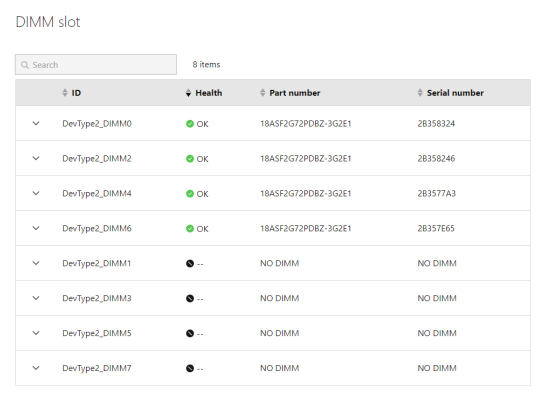
Collecting memory device configuration

The memory device configuration can be collected:

- Using the BMC Web UI
- Using Redfish

Collecting memory device configuration using the BMC Web UI

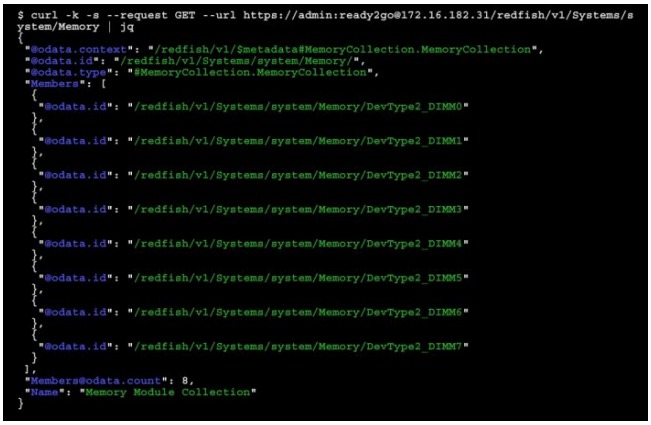
Access the BMC Web UI. Refer to Accessing a BMC using the Web UI for access instructions.

Step_1	From the left-side menu of the BMC Web UI, select **Hardware status** and then **Inventory and LEDs** .	
Step_2	From the **DIMM slot** section, collect the memory configuration information.	

Collecting memory device configuration using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	List all the memory devices using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Systems/system/Memory | jq**



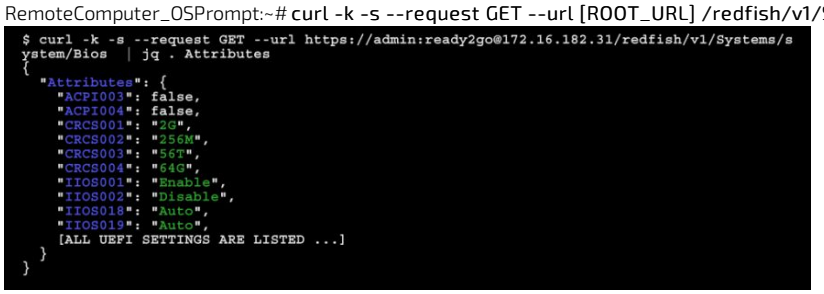
Step_2	Collect m emory device information using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Systems/system/Memory/[DEVICE_URL] | jq**

Collecting the UEFI/BIOS configuration

The UEFI/BIOS configuration can only be collected using Redfish. Refer to Accessing a BMC using Redfish for access instructions.

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
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.

Step_1	Obtain the current UEFI/BIOS settings. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Systems/system/Bios | jq .Attributes**



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.

Collecting the Ethernet switch running configuration

The Ethernet switch running configuration can be collected:

- Using the switch NOS CLI
- Using the switch NOS Web UI

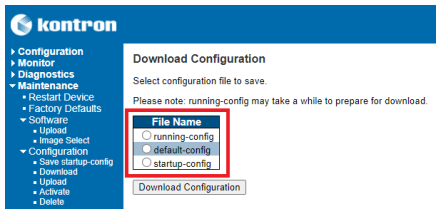
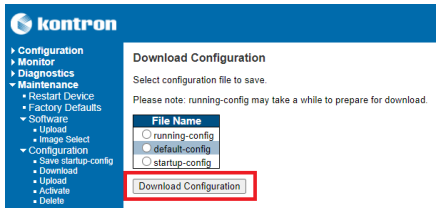
Collecting the Ethernet switch running configuration using the switch NOS CLI

Refer to Accessing the switch network operating system for access instructions.

Step_1	Access the switch network operating system using SSH or a serial connection.	
Step_2	Copy the desired configuration to the remote server. • **running-config** : Configuration currently active (may differ from startup-config if changes were made since the last boot, but not saved). • **startup-config** : Saved configuration applied at switch boot. • **default-config** : Configuration applied when the default configuration is reloaded. LocalSwitchNOS_OSPrompt:~# **copy <running-config|startup-config> scp://<SERVER_USERNAME>:<SERVER_PASSWORD>@<SERVER_IP>/<FILE_PATH> save-host-key**	# copy startup-config scp://user:password@192.168.0.10/S tartupConfig Backup save-host-key % saving 1506 bytes to server 192.168.0.10: S tartupConfig Backup

Collecting the Ethernet switch running configuration using the switch NOS Web UI

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

Step_1	From the left-side menu of the switch NOS Web UI, select **Maintenance** , then **Configuration** , and then **Download** . Choose the configuration to back up: • **running-config** : Configuration currently active (may differ from startup-config if changes were made since the last boot, but not saved). • **default-config** : Configuration applied when the default configuration is reloaded. • **startup-config** : Saved configuration applied at switch boot.	
Step_2	Click **Download Configuration** , then select where to save the configuration file.	

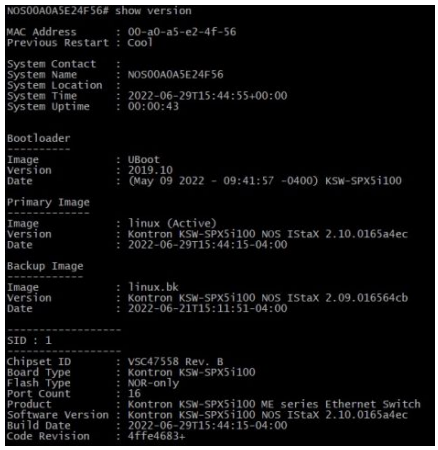
Collecting the Ethernet switch firmware version

The Ethernet switch firmware version can be collected:

- Using the switch NOS CLI
- Using switch NOS Web UI

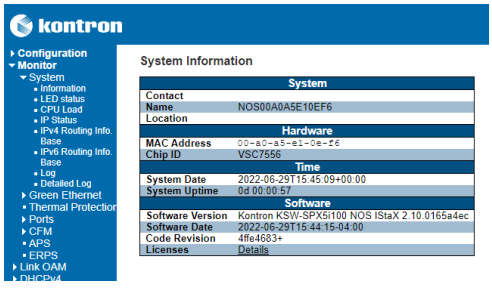
Collecting the Ethernet switch firmware version using the switch NOS CLI

Refer to Accessing the switch network operating system for access instructions.

Step_1	Display versions. LocalSwitchNOS_OSPrompt:~# **show version**	

Collecting the Ethernet switch firmware version using the switch NOS Web UI

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

Step_1	From the left-side menu, select **Monitor** , **System** and then **Information** .	

Monitoring

Monitoring sensors

Table of contents

The platform has many sensors, you can refer to the Sensor list 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

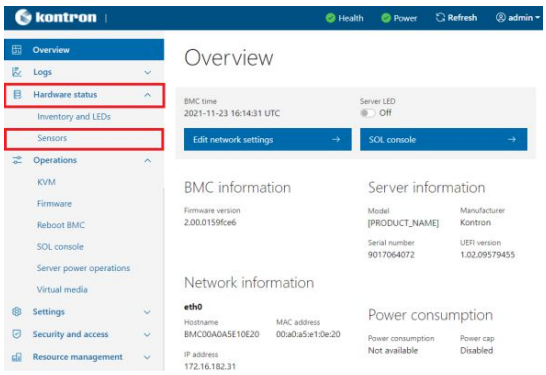
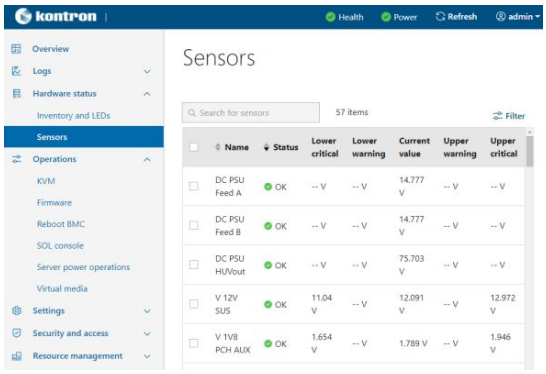
There are several methods to monitor platform sensors, including:

- Using the BMC Web UI
- Using Redfish
- Using IPMI

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

Monitoring using the BMC Web UI

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** .	
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.	

Monitoring using Redfish

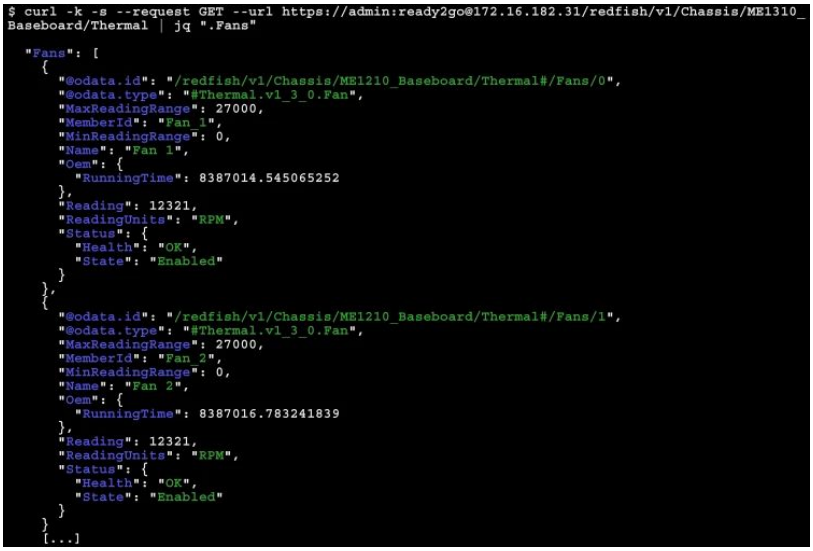
The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Creating URL extensions

For the list of all the URL extensions, refer to Sensor list . This table contains the main categories of sensors and their location.

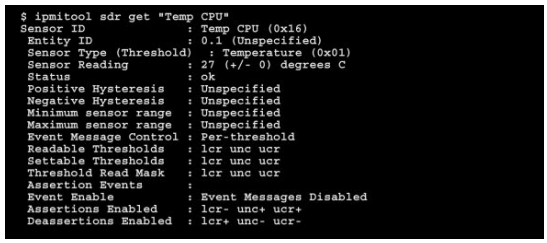
Type	URL extensions	Parser arguments
Fan sensors	Chassis/ ME1310_Baseboard /Thermal	| jq ".Fans"
Temperature sensors (including PSU sensors)	Chassis/ ME1310_Baseboard /Thermal	| jq ".Temperatures"
Voltage sensors (including PSU sensors)	Chassis/ ME1310_Baseboard /Power	| jq ".Voltages"
Power sensors (including PSU sensors)	Chassis/ ME1310_Baseboard /Sensors	| jq
Other unit-based sensors	Chassis/ ME1310_Baseboard /Sensors	| jq
Discrete sensors	Managers/bmc	| jq ".Oem.Kontron.Discrete"
Pass-through IO module sens ors	Chassis /IOBoard/Thermal	| jq ".Temperatures"
Ethernet switch IO module sensors	Chassis /Switchboard/Thermal	| jq ".Temperatures"

Viewing sensor details

Step_1	Append the root URL with the appropriate extension depending on the type of sensor. Refer to the URL extensions table above. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/[URL_EXTENTION] | [PARSER_ARGUMENT]** 

Monitoring using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -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**	
Step_2	Use the **sdr** command to see more details about a specific sensor. LocalServer_OSPrompt:~# **ipmitool sdr get [SENSOR_ID]**	

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
- TelcoAlarm1-7

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
0x01	Unexpected power loss
0x02	Power cycle or serial port reset
0x06	Cold reset
0x07	Power reset from IPMI command

Monitoring Board Reset using IPMI

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

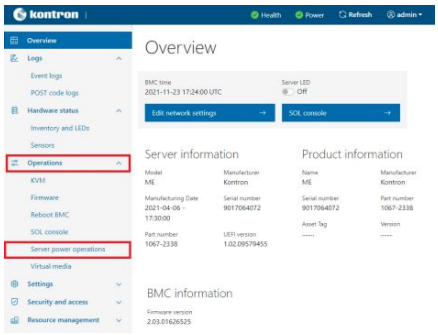
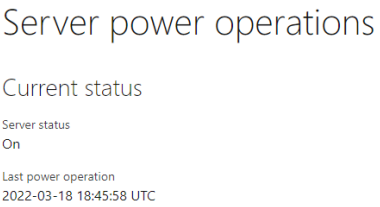
Step_1	Access the system event log and identify the ID of the desired event from the first column. LocalServer_OSPrompt:~# **ipmitool sel list**	
Step_2	Display the details of the system event log entry. LocalServer_OSPrompt:~# **ipmitool get [ID]** The value is represented by the most significant byte 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.	

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.	
Step_2	The last power operation time will be displayed.	

Monitoring the last reset time using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/ Systems/system | jq .LastResetTime** 

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 degrees Celsius
Sensor list

Possible values

Value	Description
0	Device disabled
1	Device enabled

Monitoring heaters using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish 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 -s --request GET --url [ROOT_URL]/redfish/v1/ Managers/bmc | jq .Oem.Kontron.Discrete**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1
/Managers/bmc | jq .Oem.Kontron.Discrete
{
    "Heater_CPU": "0",
    "Heater_PCIe1": "0",
    "Heater_PCIe2": "0",
    "Jumpers_Status": {
        "JMP1 (JPx p1-2)": "?",
        "JMP2 (JPx p3-4)": "OUT",
        "JMP3 (JPx p5-6)": "OUT",
        "JMP4 (JPx p7-8)": "OUT",
        "JMP5 (JPx p9-10)": "OUT",
        "JMP6 (JPx p11-12)": "OUT",
        "JMP7 (JPx p13-14)": "OUT"
    },
    "TelcoAlarm1": "1",
    "TelcoAlarm2": "1",
    "TelcoAlarm3": "1",
    "TelcoAlarm4": "1"
}
```

Monitoring heaters using IPMI

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

Step_1	Display the heaters' statuses using the following command.
	LocalServer_OSPrompt:~# **ipmitool sensor | grep Heater**
	The value is represented by the second byte from the left in the fourth column. Possible values are:
	• **0x0080** if the heater is disabled
	• **0x0180** if the heater is enabled
	• **na** if the heater is not present
		`$ ipmitool sensor | grep Heater`
		`Heater CPU | 0x0 | discrete | 0x0080 | na | na | na`
		`Heater PCIe1 | 0x0 | discrete | na | na | na | na`
		`Heater PCIe2 | 0x0 | discrete | na | na | na | na`

Intru sion

The chassis intrusion sensor will register an event (event assertion) if one of the two chassis doors (bottom hinged door or front maintenance access panel) is opened. This event will be registered in the system event log of the BMC as a critical chassis intrusion event. There is one sensor for both doors.
This sensor needs manual deassertion. When it is manually deasserted, the BMC will register a chassis intrusion reset event in the system event log. However, a reset event does not clear the BMC health status. Currently, the only supported way of restoring the BMC health status is by clearing the system event log using Redfish or the BMC Web UI (IPMI cannot be used for that purpose). Kontron recommends exporting the system event log before clearing it.

Relevant sections:
Sensor list
System event log

Monitoring the intrusion sensor using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Display the **IntrusionSensor** status using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Chassis/RS1310_Baseboard | jq .PhysicalSecurity** Possible values for **IntrusionSensor** are: • **Normal:** the contact is closed and any previous detection has been manually deasserted • **HardwareIntrusion:** the contact is open or a previous detection has not been manually deasserted

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.174.81/redfish/v1/Chassis/ME1310_
Baseboard | jq .PhysicalSecurity
{
  "IntrusionSensor": "Normal",
  "IntrusionSensorNumber": 1,
  "IntrusionSensorReArm": "Manual"
}
```

Monitoring the intrusion sensor using IPMI

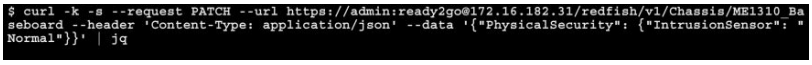
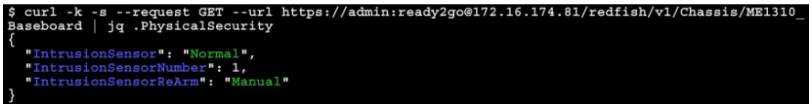
The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17** .

Step_1	Display the intrusion sensor status using the following command. LocalServer_OSPrompt:~# **ipmitool sensor | grep Intrusion** The value is represented by the second byte from the left in the fourth column. Possible values are: • **0x0180** for a closed contact • **0x0080** for an open contact	

Deasserting the Intrusion sensor

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.

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Manually change the sensor's value using the following command: RemoteComputer_OSPrompt:~# **curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Chassis/RS1310_Baseboard --header 'Content-Type: application/json' --data '{"PhysicalSecurity": {"IntrusionSensor": "Normal"}}' | jq**
	
Step_2	Check the **IntrusionSensor** status using the following command. If it is still **HardwareIntrusion** , it means one of the doors is still not properly closed and Step_3 needs to be performed. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Chassis/RS1310_Baseboard | jq .PhysicalSecurity**
	
Step_3	Make sure both doors are properly closed and perform Step_1 and then Step_2 again until the status is **Normal** .

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

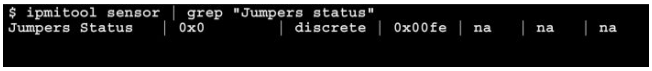
Monitoring Jumpers Status sensor using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Display the Jumpers Status sensor values using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/ Managers/bmc | jq .Oem.Kontron.Discrete**
	

Monitoring Jumpers Status sensor using IPMI

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

Step_1	Display the Jumpers Status sensor value using the following command. LocalServer_OSPrompt:~# **ipmitool sensor | grep "Jumpers Status"** The value is represented by bytes in the fourth column. The value should always be **0x00fe** .	

TelcoAlarms

TelcoAlarm sensors are normally-closed dry contacts between an **Alarm Input** signal and the **Alarm Common** signal. Those signals are located on the alarm connector. TelcoAlarms are used to detect alarm connector input statuses.
TelcoAlarm sensors will generate a TelcoAlarm event in the BMC system event log when an input changes from closed to open. In addition, the BMC health status will be set to critical. When a TelcoAlarm input changes from open to closed, the BMC will register a TelcoAlarm restoration event in the system event log. However, a restoration event does not clear the BMC health status. Currently, the only supported way of restoring the BMC health status is by clearing the system event log using Redfish or the BMC Web UI (IPMI cannot be used for that purpose). Kontron recommends exporting the system event log before clearing it.
If the alarm connector is not used, TelcoAlarm sensors should be disabled to avoid TelcoAlarm event generation in the BMC system event log when a BMC reboot occurs. This happens because in order to detect faulty wiring (for example a cut cable) the system considers an open loop as an event—and an empty alarm connector creates an open loop. Another solution would be to install a loop back connector assembly into the unused alarm connector.

There are seven TelcoAlarm sensors present in this platform (TelcoAlarm[1-7]).

Relevant sections:
Platform components (for alarm connector location)
Connector pinouts and electrical characteristics (for alarm connector pinout)
Configuring sensors and thermal parameters (to enable or disable TelcoAlarm sensors)
Sensor list
System event log

Monitoring TelcoAlarms using Redfish

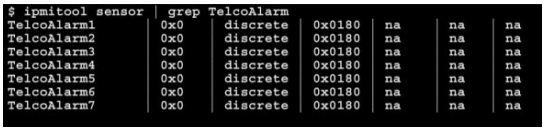
The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Display the TelcoAlarm statuses using the following command. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/ Managers/bmc | jq .Oem.Kontron.Discrete** Possible values are: • **0** for a closed contact • **1** for an open contact **NOTE:** The number of TelcoAlarms depends on the platform used. In the example below, the platform has 7.

```
$ curl -k -s --request GET https://admin:ready2go@172.16.175.208/redfish/v1/Managers/bmc | jq .O
em.Kontron.Discrete
{
  "@odata.id": "/redfish/v1/Managers/bmc#/Oem/Kontron/Discrete",
  "@odata.type": "#OemManager.Discrete",
  "Heater_CPU": "0",
  "Heater_PCIe1": "0",
  "Heater_PCIe2": "0",
  "Jumpers_Status": {
    "JMP1 (JPx p1-2)": "?",
    "JMP2 (JPx p3-4)": "OUT",
    "JMP3 (JPx p5-6)": "OUT",
    "JMP4 (JPx p7-8)": "OUT",
    "JMP5 (JPx p9-10)": "OUT",
    "JMP6 (JPx p11-12)": "OUT",
    "JMP7 (JPx p13-14)": "OUT"
  },
  "TelcoAlarm1": "1",
  "TelcoAlarm2": "1",
  "TelcoAlarm3": "1",
  "TelcoAlarm4": "1",
  "TelcoAlarm5": "1",
  "TelcoAlarm6": "1",
  "TelcoAlarm7": "1",
  "TelcoAlarm_Logging": "NO"
}
```

Monitoring TelcoAlarms using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -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 NOTE: The number of TelcoAlarms depends on the platform used. In this example, the platform has 7.	

Sensor list

Table of contents

Refer to Monitoring sensors for monitoring instructions.
For Redfish URL extensions, refer to Monitoring sensors using Redfish - Creating URL extensions.
For information about **Sensor type code** and **Event/Reading type code**, refer to Interpreting sensor data.

ME1310 sensors

ME1310 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 CPU	Internal CPU temperature	Temperature (0x01)	0x01 (Threshold Based)
Temp BMC	Temperature under BMC	Temperature (0x01)	0x01 (Threshold Based)
Temp CPU Area	Temperature under CPU	Temperature (0x01)	0x01 (Threshold Based)
Temp Chassis	Temperature from chassis thermistor Refer to Installing a thermal probe for the PCIe add-in card for thermal probe location.	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMA1	Temperature of DIMM 1 on channel A	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMA2	Temperature of DIMM 2 on channel A	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMB1	Temperature of DIMM 1 on channel B	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMB2	Temperature of DIMM 2 on channel B	Temperature (0x01)	0x01 (Threshold Based)

Temp DIMMC1	Temperature of DIMM 1 on channel C	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMC2	Temperature of DIMM 2 on channel C	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMD1	Temperature of DIMM 1 on channel D	Temperature (0x01)	0x01 (Threshold Based)
Temp DIMMD2	Temperature of DIMM 2 on channel D	Temperature (0x01)	0x01 (Threshold 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 Area	Temperature near M.2 J8 and J9	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 1	Temperature from PCIe slot 1 thermistor Refer to Installing a thermal probe for the PCIe add-in card for thermal probe location.	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 1 mbox	Temperature from PCIe slot 1 reported via mailbox Refer to Platform resources for customer application - Customer-specific temperature sensors for reporting instructions.	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 2	Temperature from PCIe slot 2 thermistor Refer to Installing a thermal probe for the PCIe add-in card for thermal probe location.	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 2 mbox	Temperature from PCIe slot 2 reported via mailbox Refer to Platform resources for customer application - Customer-specific temperature sensors for reporting instructions.	Temperature (0x01)	0x01 (Threshold Based)
Temp PSU Outlet	Temperature of system PSU outlet	Temperature (0x01)	0x01 (Threshold Based)
Temp VCCIN	Temperature near VCCIN switcher	Temperature (0x01)	0x01 (Threshold Based)
Temp VDDQ_AB	Temperature near VDDQ_AB switcher	Temperature (0x01)	0x01 (Threshold Based)
Temp VDDQ_CD	Temperature near VDDQ_CD switcher	Temperature (0x01)	0x01 (Threshold Based)
Temp V_3V3_SUS	Temperature near V_3V3_SUS switcher	Temperature (0x01)	0x01 (Threshold 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_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_RGM_BMC	V_3V3_RGM_BMC 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_CD	V_VTT_CD 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)
TelcoAlarm5	Status from front panel alarm connector	Platform Alert (0x24)	0x3 ('digital' Discrete - Assert/Deassert)
TelcoAlarm6	Status from front panel alarm connector	Platform Alert (0x24)	0x3 ('digital' Discrete - Assert/Deassert)
TelcoAlarm7	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) (0xC4)	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 ME1310 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 output voltage	Voltage (0x02)	0x01 (Threshold Based)
DC PSU Iout	DC PSU 48V to 12V regulator output 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 Temp3p0	PSU 'Main output HotSpot (Secondary side)' temperature	Temperature (0x01)	0x01 (Threshold Based)

	(Temp3p0 is for: PMBUS READ_ **TEMPERATURE_3** (0x8F) command **page 0**)		

IO module sensors

The IO module sensors will differ according to the IO module configuration of the platform.

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 p ass-through IO module module.
This option is planned for development. Please contact Kontron sales .

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>	Local temperature for Silicom P3iMB PCIe add-in card Where <X> is the PCIe slot ID.	Temperature (0x01)	0x01 (Threshold Based)
T ACC100 TSDE S<X>	Intel ACC100 FEC accelerator TSDE East temperature for Silicom P3iMB PCIe add-in card Where <X> is the PCIe slot ID.	Temperature (0x01)	0x01 (Threshold Based)
T ACC100 TSDW S<X>	Intel ACC100 FEC accelerator TSDW West temperature for Silicom P3iMB PCIe add-in card Where <X> is the PCIe slot ID.	Temperature (0x01)	0x01 (Threshold Based)

Maintenance

System event log

Table of contents

BMC system event logs

System event logs can be accessed:

- Using the BMC Web UI
- Using Redfish
- Using IPMI

Relationship between BMC system event logs

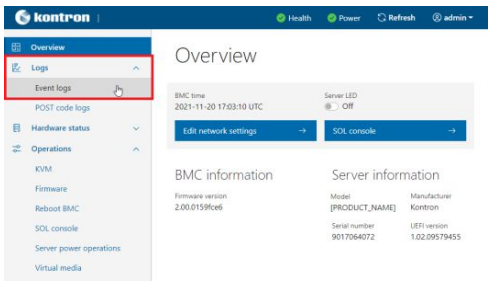
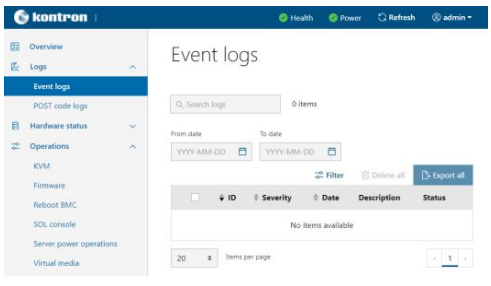
System event logs accessed via the BMC Web UI and Redfish are managed independently. This has two implications:

- 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.

Accessing the BMC SEL using the BMC Web UI

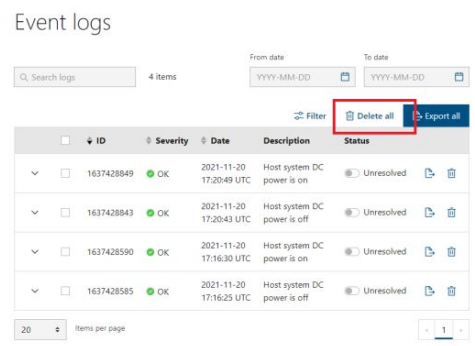
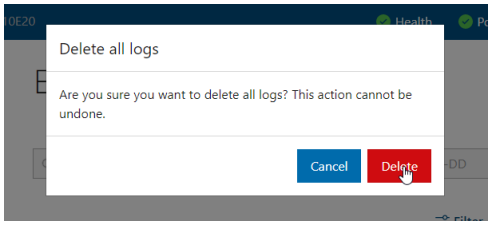
Refer to Accessing a BMC using the Web UI for access instructions.

Accessing the BMC system event log

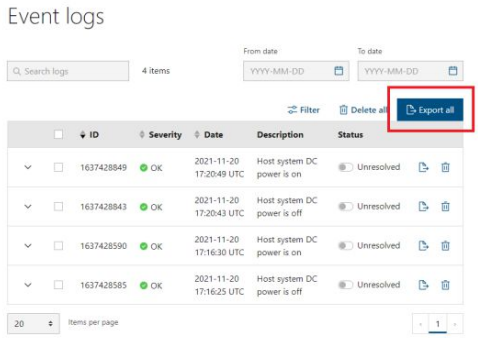
Step_1	From the left-side menu of the BMC Web UI, select **Logs** and then **Event Logs** .	
Step_2	The system event log is displayed. The following information can be collected: 1. Event ID 2. Severity 3. Date 4. Description 5. Status	

Clearing the BMC 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.	
Step_2	Confirm choice by clicking on the **Delete** button.	

Exporting the BMC system event log

Step_1	Click on the **Export all** button to download the system event log.	

Accessing the BMC SEL using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Accessing the BMC system event log

NOTE: Depending on the event, there may not be an associated sensor attribute. However, if this attribute is present, refer to Interpreting sensor data for further interpretation instructions.

Step_1	From a remote computer that has access to the management network subnet, open a command prompt and a ccess the system event log. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system/LogServices/EventLog/Entries | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/
LogServices/EventLog/Entries  | jq
{
  "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries",
  "@odata.type": "#LogEntryCollection.LogEntryCollection",
  "Description": "Collection of System Event Log Entries",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries/1647629153",
      "@odata.type": "#LogEntry.v1_4_0.LogEntry",
      "Created": "2022-03-18T18:45:53+00:00",
      "EntryType": "Event",
      "Id": "1647629153",
      "Message": "Host system DC power is off",
      "MessageArgs": [],
      "MessageId": "OpenBMC.0.1.DCPowerOff",
      "Name": "System Event Log Entry",
      "Severity": "OK"
    },
    {
      "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries/1647629154",
      "@odata.type": "#LogEntry.v1_4_0.LogEntry",
      "Created": "2022-03-18T18:45:54+00:00",
      "EntryType": "Event",
      "Id": "1647629154",
      "Message": "System Restart : Normal power down",
      "MessageArgs": [
        "Normal power down"
      ],
      "MessageId": "OpenBMC.0.1.BoardReset",
      "Name": "System Event Log Entry",
      "Severity": "OK"
    },
[...]
```

Step_2	If there are more than 1000 entries in the log, the command in Step_1 will add a link describing how to output the next entries at the end of the response:

```
$ curl -k -s --request GET --url 'https://admin:ready2go@169.254.0.17/redfish/v1/Systems/system/LogServices/Ev
entLog/Entries' | jq '.["Members@odata.nextLink"]'
"/redfish/v1/Systems/system/LogServices/EventLog/Entries?$skip=1000"
```

RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url ' [ROOT_URL]/redfish/v1/Systems/system/LogServices/EventLog/Entries?$skip=1000' | jq**
NOTE: The URL in the command above may need to be in single quotes as in the example, e.g. '...'
This is to avoid shell expansion.

Clearing the BMC 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 -s --request POST --url [ROOT_URL] /redfish /v1/Systems/system/LogServices/EventLog/Actions/LogService.ClearLog | jq**

```
$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system
/LogServices/EventLog/Actions/LogService.ClearLog  | jq
{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "Successfully Completed Request",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Success",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

Step_2	Verify that the system event log was properly cleared. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL] /redfish /v1/Systems/system/LogServices/EventLog/Entries | jq**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/
LogServices/EventLog/Entries  | jq
{
  "@odata.id": "/redfish/v1/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"
}
```

Redfish supported event types

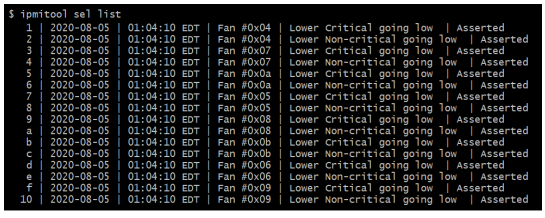
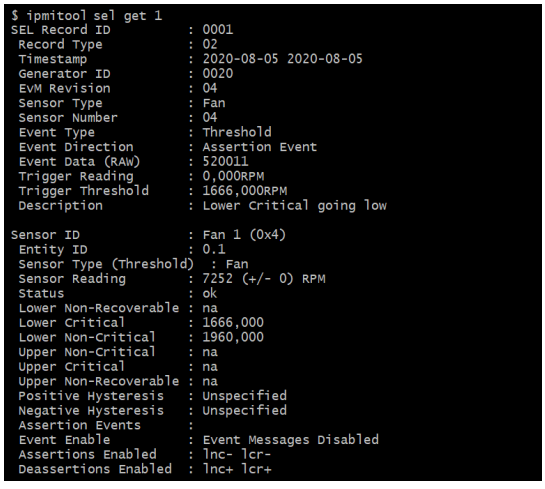
The event format is composed of the OpenBMC event schema version followed by the event type [SCHEMA VERSION].[EVENT TYPE].
The current schema version is **OpenBMC.0.1** .

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
TelcoAlarmDetected	Indicates that a TelcoAlarm has been detected
ChassisIntrusionDetected	Indicates that a chassis intrusion has been detected
HeaterStatusEnabled	Indicates that the specified heater has been activated. The specific heater is given in the "Message" object. Example: "Message": "Heater_CPU : Device Enabled"
HeaterStatusDisabled	Indicates that the specified heater has been deactivated. The specific heater is given in the "Message" object. Example: "Message": "Heater_CPU : Device Disabled"

Accessing the BMC SEL using IPMI

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

Accessing the BMC system event log

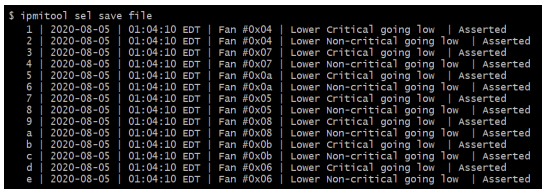
Step_1	List all the events. LocalServer_OSPrompt:~# **ipmitool sel list**	
Step_2	To obtain more details about a specific event, use the following command. LocalServer_OSPrompt:~# **ipmitool sel get [EVENT_ID]**	

Clearing the BMC system event log

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**	

Exporting the BMC system event log

Step_1	Use the following command to save the system event log into a file. LocalServer_OSPrompt:~# **ipmitool sel save [FILE_NAME]**	

TelcoAlarms registered in the SEL upon BMC reboot

TelcoAlarms are used to detect alarm connector input s tatuses. If nothing is connected to the alarm connector, TelcoAlarm events will be registered in the system event log (SEL) if a BMC reboot occurs. This happens because in order to detect faulty wiring (for example a cut cable) the system considers an open loop as an event—and an empty alarm connector creates an open loop.
If the alarm connector is not used, TelcoAlarm sensors should be disabled. Another solution would be to install a loop back connector assembly into the alarm connector.
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 SEL. Kontron recommends exporting the SEL before clearing it.

Relevant sections:
Platform components (for alarm connector location)
Connector pinouts and electrical characteristics (for alarm connector pinout)
Configuring sensors and thermal parameters (to enable or disable TelcoAlarm sensors)
Monitoring sensors (to view TelcoAlarm sensor statuses)

NOS system event log

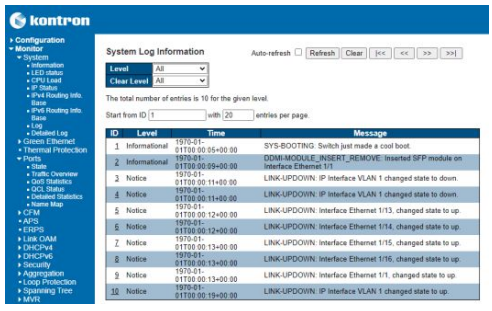
The NOS system event log can be accessed:

- Using the NOS Web UI
- Using the NOS CLI

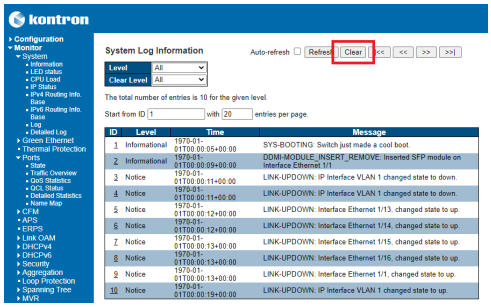
Accessing the NOS SEL using the NOS Web UI

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

Accessing the NOS system event log

Step_1	From the left-side menu, select **Monitoring** , **System** , and then **Log.** The NOS system event log should be displayed.	

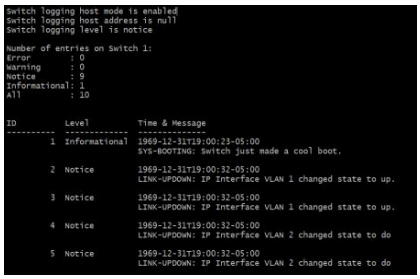
Clearing the NOS system event log

Step_1	From the left-side menu, select **Monitoring** , **System** , and then **Log**. The NOS system event log should be displayed.	
Step_2	Click on the **Clear** button.	
Step_3	The NOS system event log should be empty.	

Accessing the NOS SEL using the NOS CLI

Refer to Accessing the switch NOS for access instructions.

Accessing the NOS system event log

Step_1	Display the switch NOS event log. LocalSwitchNOS_OSPrompt:~# **show logging**	

Clearing the NOS system event log

Step_1	Display the switch NOS event log. LocalSwitchNOS_OSPrompt:~# **clear logging**
Step_2	The NOS system event log should be empty. LocalSwitchNOS_OSPrompt:~# **show logging**

```
NOS00A0A5E10EF6# clear logging
NOS00A0A5E10EF6# show logging
Switch logging host mode is disabled
Switch logging host address is null
Switch logging level is informational

Number of entries on Switch 1:
Error        : 0
Warning      : 0
Notice       : 0
Informational: 0
All          : 0

NOS00A0A5E10EF6#
```

Interpreting sensor data

Table of contents

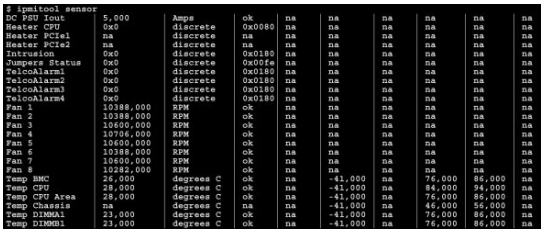
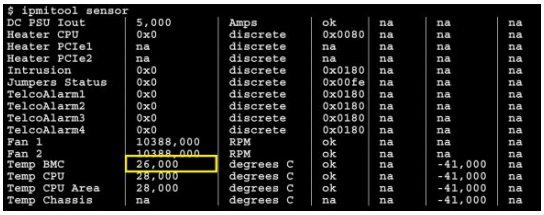
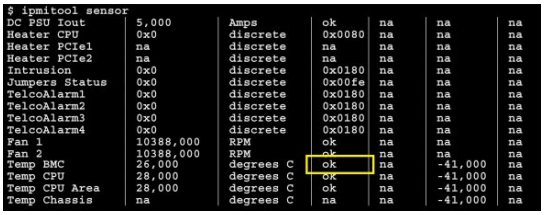
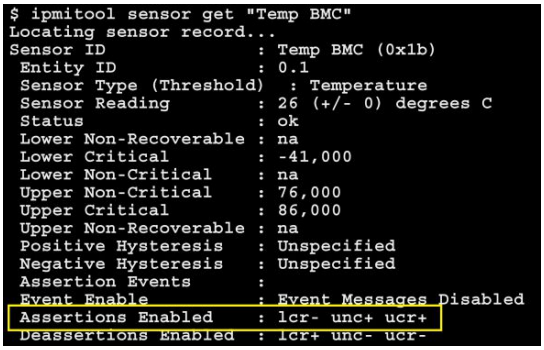
Interpretation procedure

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

- Event ID
- Associated sensor
- Description

Refer to System event log for instructions.

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

Step_1	In **ipmitool** , the **sensor** command returns a table. LocalServer_OSPrompt:~# **ipmitool sensor** The columns are defined as: • Name • Numerical reading • Event/reading type/unit • Unit-based sensors status/discrete sensors reading • Lower non-recoverable threshold value • Lower critical threshold value • Lower noncritical threshold value • Upper noncritical threshold value • Upper critical threshold value • Upper non-recoverable threshold value	
Step_2	The numerical reading value is shown in the second column. LocalServer_OSPrompt:~# **ipmitool sensor**	
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 **OK**. Otherwise, the last threshold reached is displayed. Refer to Threshold-based event and reading type for the definitions of threshold states.	
Step_4	An event will be created according to the assertion enabled for the specified sensor. LocalServer_OSPrompt:~# **ipmitool sensor get "[SENSOR_ID]"**	

Interpretation information

Each sensor has a Sensor type attribute and a Sensor event and reading type attribute. For more information about IPMI sensors refer to the IPMI 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.
C4h (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 and 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 Threshold-based event and reading type table

Threshold-based event and 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	

POST code logs

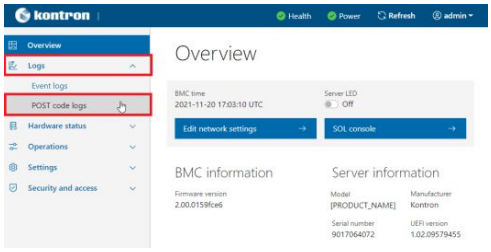
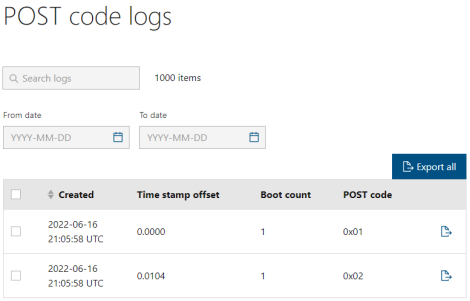
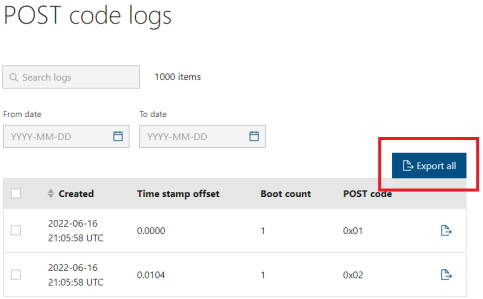
Table of contents

The POST codes can be accessed:

- Using the BMC Web UI
- Using Redfish

Accessing the POST code logs using the BMC Web UI

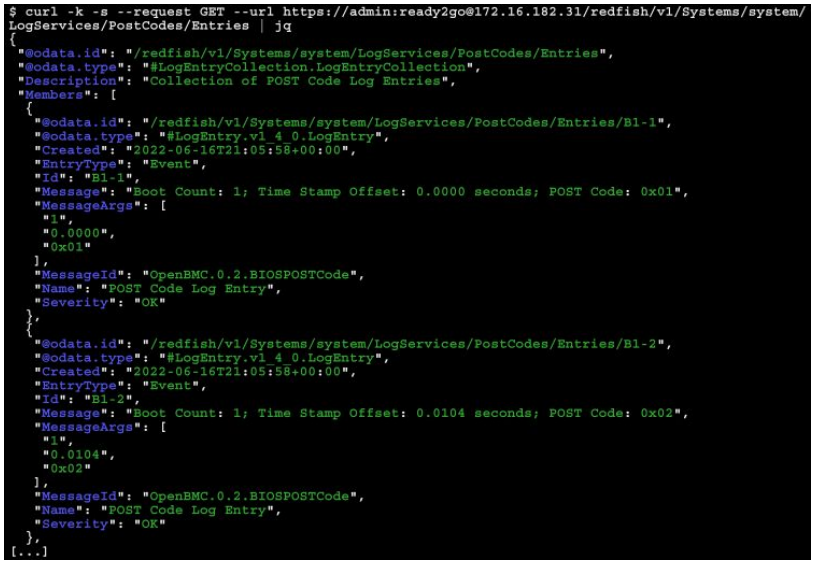
Refer to Accessing a BMC using the Web UI for access instructions.

Step_1	From the left-side menu of the BMC Web UI, select **Logs** and then **POST code logs** .	
Step_2	The system event log is displayed. The following information can be collected: 1. Event ID 2. Time stamp offset 3. Boot count 4. POST code 5. Status	
Step_3	Click on **Export all** to download the POST code logs.	

Accessing the POST code logs using Redfish

The following procedures will be executed using the Redfish ROOT URL required for an external network connection. They can also be executed using the Redfish ROOT URL required for the internal Redfish host interface if the commands are initiated locally from the server operating system.
Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Access the POST code logs using the following command. RemoteComputer_OSPrompt:~# **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system/LogServices/PostCodes/Entries | jq**



```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system/
LogServices/PostCodes/Entries | jq
{
 "@odata.id": "/redfish/v1/Systems/system/LogServices/PostCodes/Entries",
 "@odata.type": "#LogEntryCollection.LogEntryCollection",
 "Description": "Collection of POST Code Log Entries",
 "Members": [
  {
   "@odata.id": "/redfish/v1/Systems/system/LogServices/PostCodes/Entries/B1-1",
   "@odata.type": "#LogEntry.v1_4_0.LogEntry",
   "Created": "2022-06-16T21:05:58+00:00",
   "EntryType": "Event",
   "Id": "B1-1",
   "Message": "Boot Count: 1; Time Stamp Offset: 0.0000 seconds; POST Code: 0x01",
   "MessageArgs": [
    "1",
    "0.0000",
    "0x01"
   ],
   "MessageId": "OpenBMC.0.2.BIOSPOSTCode",
   "Name": "POST Code Log Entry",
   "Severity": "OK"
  },
  {
   "@odata.id": "/redfish/v1/Systems/system/LogServices/PostCodes/Entries/B1-2",
   "@odata.type": "#LogEntry.v1_4_0.LogEntry",
   "Created": "2022-06-16T21:05:58+00:00",
   "EntryType": "Event",
   "Id": "B1-2",
   "Message": "Boot Count: 1; Time Stamp Offset: 0.0104 seconds; POST Code: 0x02",
   "MessageArgs": [
    "1",
    "0.0104",
    "0x02"
   ],
   "MessageId": "OpenBMC.0.2.BIOSPOSTCode",
   "Name": "POST Code Log Entry",
   "Severity": "OK"
  },
[...]
```

Component replacement

Refer to Components installation and assembly for component replacement procedures.

Backup and restore

Table of contents

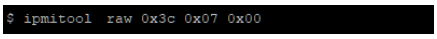
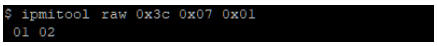
On an ME1310 platform, UEFI/BIOS firmware and settings as well as integrated switch NOS configurations can be backed up and restored.

UEFI/BIOS firmware and setting backup

This section describes how to create a UEFI/BIOS firmware backup that includes the current UEFI/BIOS user settings and perform a restore from the backup created.
The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17** .

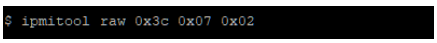
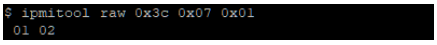
Backing up the UEFI/BIOS

For information on [BYTE1] , refer to Description of creation and restoration steps .

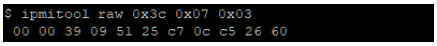
Step_1	Back up the UEFI/BIOS. This action saves the UEFI/BIOS and the configuration. LocalServer_OSPrompt: ~# **ipmitool raw 0x3c 0x07 0x00** Completion code: • 0x00: Recovery process started successfully • 0xd5: Recovery process cannot be started	
Step_2	Verify the UEFI/BIOS backup status. LocalServer_OSPrompt: ~# **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 backup creation is **In-progress** and the current step is **Set Server to Power Off state.**	

Restoring the UEFI/BIOS

For information on [BYTE1] , refer to Description of creation and restoration steps .

Step_1	Restore the UEFI/BIOS. This action restores the UEFI/BIOS and the configuration. LocalServer_OSPrompt: ~# **ipmitool raw 0x3c 0x07 0x02** Completion code: • 0x00: Recovery process started successfully • 0xd5: Recovery process cannot be started	
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.**	

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** .	

Description of creation and restoration steps

Step description	Step value (BYTE1)	Details
No step	0x00	Nothing is currently going on, no failure to report.
Get UEFI/BIOS version	0x01	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	0x05	Target flash being erased. Target depends on whether action is CREATE or RESTORE.
MTD Flash write	0x06	Target flash being written. Target depends on whether action is CREATE or RESTORE.
MTD Flash verify	0x07	Target flash being verified. Target depends on whether action is CREATE or RESTORE.
Reset Intel ME to Normal mode	0x08	Reset Intel ME to return to normal mode.
Server Power On	0x09	Set server to Power On state.

Switch NOS configuration

This section describes how to backup and restore the switch NOS configuration.
NOTE: To restore the factory default configuration, refer to Factory default .

Backing up the switch NOS configuration

This operation can be achieved:
- Using SCP
- Using the switch NOS Web UI

Backing up the switch NOS configuration using SCP

Prerequisites

1	A server configured for the desired protocol is available and accessible from the switch NOS.

	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>).

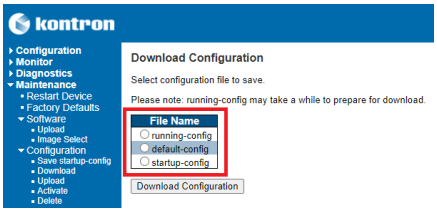
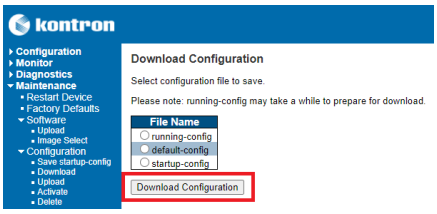
Procedure

Refer to Accessing the switch network operating system for access instructions.

Step_1	Access the switch network operating system using SSH or a serial connection.	
Step_2	Copy the desired configuration to the remote server. • **running-config** : Configuration currently active (may differ from startup-config if changes were made since the last boot, but not saved). • **startup-config** : Saved configuration applied at switch boot. • **default-config** : Configuration applied when the default configuration is reloaded. LocalSwitchNOS_OSPrompt:~# **copy <running-config|startup-config> scp://<SERVER_USERNAME>:<SERVER_PASSWORD>@<SERVER_IP>/<FILE_PATH> save-host-key**	# copy startup-config scp://user:password@192.168.0.10/S tartupConfig Backup save-host-key % saving 1506 bytes to server 192.168.0.10: S tartupConfig Backup

Backing up the switch NOS configuration using the switch NOS Web UI

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

Step_1	From the left-side menu of the switch NOS Web UI, select **Maintenance** , then **Configuration** , and then **Download** . Choose the configuration to back up: • **running-config** : Configuration currently active (may differ from startup-config if changes were made since the last boot, but not saved). • **default-config** : Configuration applied when the default configuration is reloaded. • **startup-config** : Saved configuration applied at switch boot.	
Step_2	Click **Download Configuration** , then select where to save the configuration file.	

Restoring the switch NOS configuration

This operation can be achieved:

- Using SCP
- Using the switch NOS Web UI

Relevant section:
Network switch configuration load error messages (to troubleshoot error messages associated with a restore procedure)

If error messages are generated when restoring the switch NOS configuration or upgrading its firmware, refer to the Troubleshooting section.

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>).

Procedure

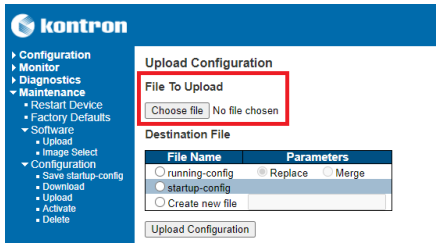
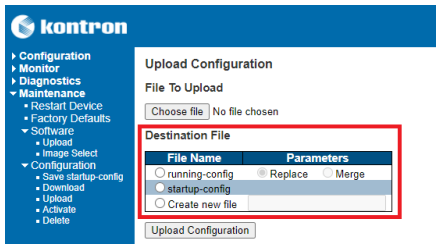
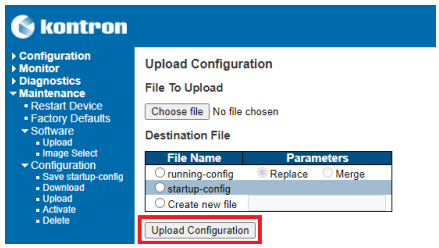
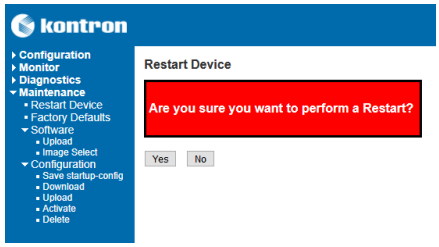
Refer to Accessing the switch network operating system for access instructions.

Step_1	Access the switch network operating system using SSH or a serial connection.	
Step_2	Copy the configuration file from the remote server specifying the destination file, which can be one of the following: • **running-config** : Configuration currently active (volatile until saved as startup-config). • **startup-config** : Saved configuration applied at switch boot. LocalSwitchNOS_OSPrompt:~# **copy scp://<SERVER_USERNAME>:<SERVER_PASSWORD>@ <SERVER_IP>/<FILE_PATH> <running-config|startup-config> save-host-key**	# copy scp://user:password@192.168.0.10/StartupConfigBackup 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:~# **reload cold**	# reload cold % Cold reload in progress, please stand by.

Restoring the switch configuration using the switch NOS Web UI

If the procedure generates error messages, they will not be shown in the switch NOS Web UI. They are only visible from a CLI interface.

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

Step_1	From the left-side menu of the switch NOS Web UI, select **Maintenance** , then **Configuration** , and then **Upload** . Click **Choose file** . Then, using the pop-up file browser, select the desired configuration file to restore.	
Step_2	Choose the configuration to restore: • **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. • **startup-config** : saved configuration applied at switch boot. • **Create new file** : creates a new configuration entry that can be subsequently activated using the **Maintenance** → **Configuration** → **Activate** path of the menu. **NOTE:** A default-config cannot be written to, but a previously backed up default-config can be written to as one of these options.	
Step_3	Click **Upload Configuration** .	
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 **Maintenance** , then **Restart Device** from the left-side menu. Then, confirm that a restart is to be performed by clicking **Yes** .	

Upgrading

Table of contents

Upgrading BMC firmware

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 firmware can be upgraded:
- Using Redfish
- Using the Web UI

Upgrading the firmware of the BMC using Redfish

Redfish is the preferred interface for upgrading BMC firmware.

Prerequisites

1	The **.tar** file provided by Kontron was downloaded on the remote computer.
2	Access to the BMC Redfish interface is required.

Relevant section:
Accessing a BMC using Redfish

Procedure

Step_1	From the BMC Redfish interface, verify the current firmware version of the BMC firmware. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc | jq .FirmwareVersion**

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc  |
 jq .FirmwareVersion
"2.00.0159fce6"
```

Step_2	Collect the list of IDs of all the firmware present on the platform. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/UpdateService/FirmwareInventory | jq .Members

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/F
irmwareInventory | jq .Members
[
  {
    "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/8c50fd55"
  },
  {
    "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/c172d3d8"
  },
  {
    "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/d6bcd2a6"
  },
  {
    "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ebbd5d7b"
  }
]
```

Step_3	Verify that the new firmware is not already on the platform. Repeat the following command for every firmware discovered in the previous step. The **Description** field describes the component targeted by this firmware. The **Version** field describes the firmware version of this component. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/UpdateService/FirmwareInventory/[FIRMWARE_ID] | jq ".Description,.Version"

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/F
irmwareInventory/c172d3d8| jq ".Description,.Version"
"BMC image"
"2.07.0162fd0d"
```

Step_4	Set the apply time to **Immediate** . RemoteComputer_OSPrompt:~$ curl -k -s --request PATCH --url [ROOT_URL] /redfish/v1/UpdateService --header 'Content-Type: application/json' --data '{"HttpPushUriOptions": {"HttpPushUriApplyTime": {"ApplyTime": " Immediate "}}}' | jq

```
$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService
 --header 'Content-Type: application/json' --data '{"HttpPushUriOptions": {"HttpPushUriApplyTime
": {"ApplyTime": "Immediate"}}}' | jq
```

Step_5	Upload the firmware by executing the following command. The BMC should return a TaskService **Id** . RemoteComputer_OSPrompt:~$ curl -k -s --request POST --url [ROOT_URL] /redfish/v1/UpdateService --header 'Content-Type: application/octet-stream' --upload-file ' [FILE_PATH]' | jq

```
$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService
--header 'Content-Type: application/octet-stream' --upload-file 'update.tar' | jq
{
 "@odata.id": "/redfish/v1/TaskService/Tasks/1",
 "@odata.type": "#Task.v1_4_3.Task",
 "Id": "1",
 "TaskState": "Running",
 "TaskStatus": "OK"
}
```

Step_6	Using the **Id** returned by the previous step, ensure that the task is completed. The **PercentComplete** value should be 100 before proceeding with the next steps. It may take several seconds. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL] /redfish/v1/TaskService/Tasks/[TASK_ID] | jq .PercentComplete

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/TaskService/Tas
ks/1  | jq .PercentComplete
[
 100
]
```

Step_7	Once the BMC becomes available again, verify that the firmware version has changed. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc | jq .FirmwareVersion

```
$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc  |
 jq .FirmwareVersion
"2.00.015afd1b"
```

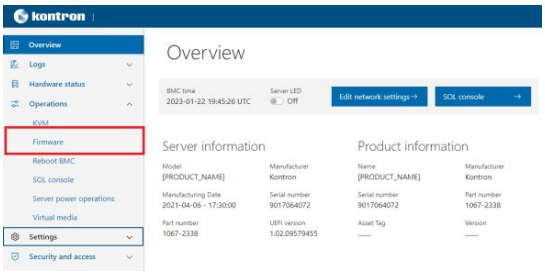
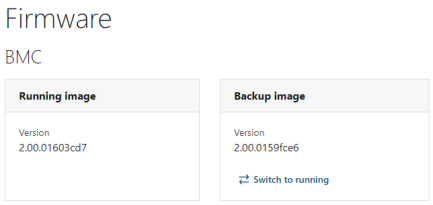
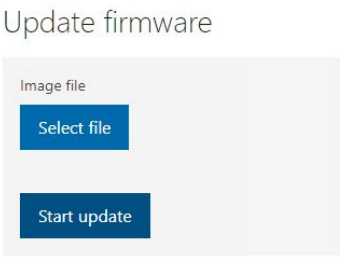
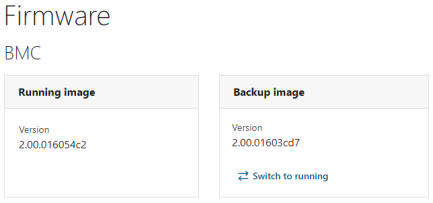
Upgrading the firmware of the BMC using the Web UI

Prerequisites

1	The **.tar** file provided by Kontron was downloaded on the remote computer.
2	Access to the BMC Web UI is required.

Relevant section:
Accessing a BMC using the Web UI

Procedure

Step_1	From the left-side menu of the BMC Web UI, click on **Operations** and then on **Firmware** .	
Step_2	Verify the current firmware version. Make sure that the new firmware is more recent.	
Step_3	From the **Update firmware** section, choose a **.tar** file to upload for the BMC by clicking on **Select file** .	
Step_4	Click on **Start update** .	
Step_5	When the file has successfully been uploaded, a success message should appear in the top right corner.	
Step_6	Wait for the BMC to update. The page should refresh automatically upon successful update.	
Step_7	Once the BMC becomes available again, verify that the firmware version has changed.	

Upgrading FPGA firmware

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

FPGA firmware can be upgraded:

- Using Redfish
- Using the Web UI

Upgrading the firmware of the FPGA using Redfish

Redfish is the preferred interface for upgrading the FPGA firmware.

Prerequisites

1	The .tar file provided by Kontron was downloaded on the remote computer.
2	Access to the BMC Redfish interface is required.

Relevant section:
Accessing a BMC using Redfish

Procedure

Step_1	From the BMC Redfish interface, verify the current FPGA firmware version.
	RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system | jq .FpgaVersion
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/System`
	`  | jq .FpgaVersion`
	`"1.00.0159fce6"`

Step_2	Collect all the IDs of the firmware present on the platform.
	RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/UpdateService/FirmwareInventory | jq .Members
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/F`
	`irmwareInventory | jq .Members`
	`[`
	`  {`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/8c50fd55"`
	`  },`
	`  {`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/c172d3d8"`
	`  },`
	`  {`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/d6bcd2a6"`
	`  },`
	`  {`
	`  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ebbd5d7b"`
	`  }`
	`]`

Step_3	Verify that the new firmware is not already on the platform. Repeat the following command for every firmware discovered in the previous step.
	The Description field describes the component targeted by this firmware.
	The Version field describes the firmware version of this component.
	RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/UpdateService/FirmwareInventory/[FIRMWARE_ID] | jq ".Description,.Version"
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/F`
	`irmwareInventory/c172d3d8| jq ".Description,.Version"`
	`"BMC image"`
	`"2.07.0162fd0d"`

Step_4	Set the apply time to Immediate .
	RemoteComputer_OSPrompt:~$ curl -k -s --request PATCH --url [ROOT_URL] /redfish/v1/UpdateService --header 'Content-Type: application/json' --data '{"HttpPushUriOptions": {"HttpPushUriApplyTime": {"ApplyTime": " Immediate "}}}' | jq
	`$ curl -k -s --request PATCH --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService`
	`  --header 'Content-Type: application/json' --data '{"HttpPushUriOptions": {"HttpPushUriApplyTime`
	`": {"ApplyTime": "Immediate"}}}' | jq`

Step_5	Upload the firmware by executing the following command. The BMC will shut down temporarily.
	RemoteComputer_OSPrompt:~$ curl -k -s --request POST --url [ROOT_URL] /redfish/v1/UpdateService --header 'Content-Type: application/octet-stream' --upload-file ' [FILE_PATH]' | jq
	`$ curl -k -s --request POST --url https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService`
	`--header 'Content-Type: application/octet-stream' --upload-file 'update.tar' | jq`
	`{`
	`  "@odata.id": "/redfish/v1/TaskService/Tasks/1",`
	`  "@odata.type": "#Task.v1_4_3.Task",`
	`  "Id": "1",`
	`  "TaskState": "Running",`
	`  "TaskStatus": "OK"`
	`}`

Step_6	Once the BMC becomes available again, verify that the firmware version has changed.
	RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system | jq .FpgaVersion
	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.182.31/redfish/v1/Systems/System`
	`  | jq .FpgaVersion`
	`"1.00.0159fce6"`

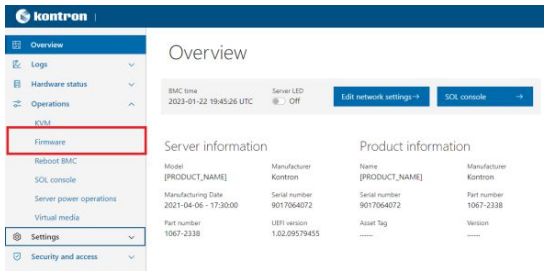
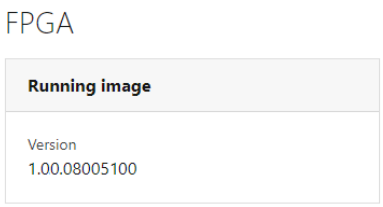
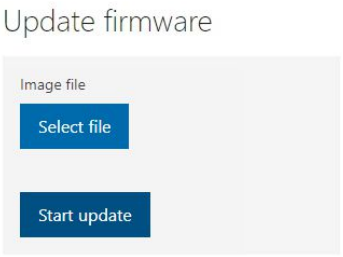
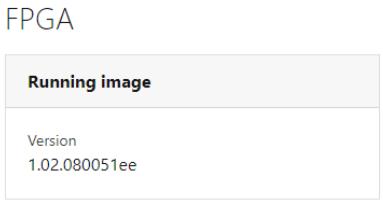
Upgrading the firmware of the FPGA using the Web UI

Prerequisites

1	The .tar file provided by Kontron was downloaded on the remote computer.
2	Access to the BMC Web UI is required.

Relevant section:
Accessing a BMC using the Web UI

Procedure

Step_1	From the left-side menu of the BMC Web UI, click on **Operations** and then on **Firmware** .	
Step_2	Verify the current firmware version. Make sure that the new firmware is more recent.	
Step_3	From the **Update firmware** section, choose a **.tar** file to upload for the FPGA by clicking on **Select file** .	
Step_4	Click on **Start update** .	
Step_5	When the file has successfully been uploaded, a success message should appear in the top right corner.	
Step_6	Wait for the FPGA to update. The page should refresh automatically upon successful update.	
Step_7	Once the FPGA becomes available again, verify that the firmware version has changed.	

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 the server operating system
- Using the Web UI
- Using Redfish

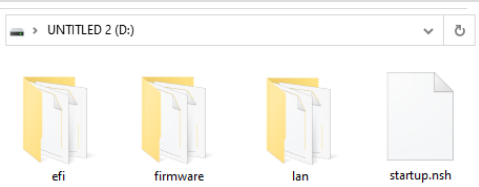
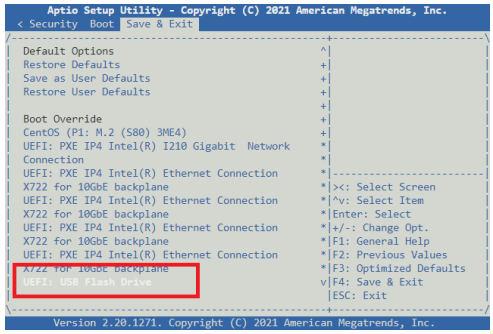
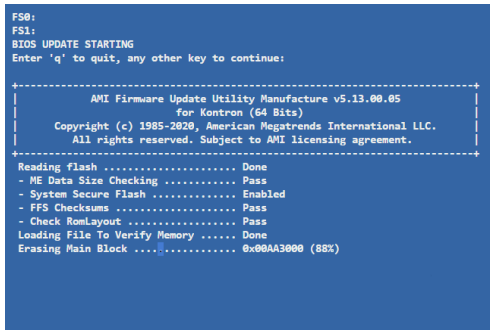
Upgrading the UEFI/BIOS firmware using the built-in UEFI shell and a USB storage device

Prerequisites

1	The **.zip** archive provided by Kontron has been downloaded.
2	Access to the UEFI/BIOS menu is required.
3	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 **startup.nsh** file should be located directly in the root folder of the USB storage device. **NOTE:** Some of the archive content can change depending on the upgrade version.	
Step_2	Insert the USB storage device in one of the USB ports of the front panel.	
Step_3	Power on the platform or reboot the integrated server. Access the UEFI/BIOS setup menu.	
Step_4	Navigate to the **Save & Exit** menu and then to the **Boot Override** section. Select the option that represents the USB storage device and press **Enter** . The built-in EFI Shell should launch.	
Step_5	Press any key other than '**q**' to continue. The UEFI/BIOS upgrade should start.	
Step_6	Once completed, the BMC and the platform will automatically reboot. It may take several seconds to complete the power cycle and the remote connection might be lost.	

Upgrading the UEFI/BIOS firmware using the built-in UEFI shell and a UEFI-compatible operating system

Prerequisites

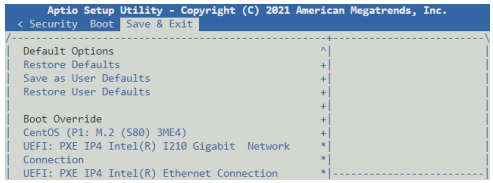
1	The **.zip** archive provided by Kontron has been downloaded.
2	Access to the UEFI/BIOS menu is required.
3	A Linux UEFI-compatible operating system is installed on the platform.
4	Access to the OS is required.

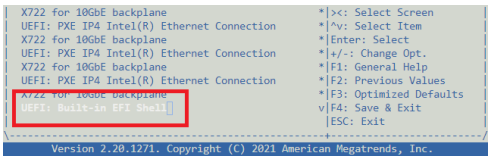
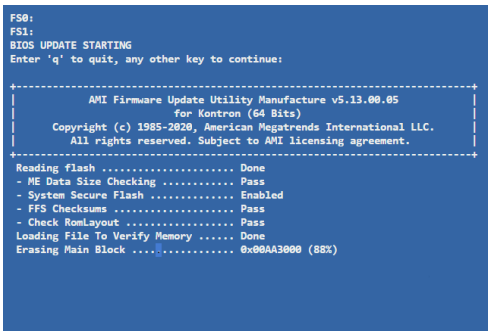
Relevant sections:
Accessing the UEFI or BIOS
Accessing the operating system of a server

Procedure

Step_1	P ower on the platform or reboot the integrated server. Access the operating system.	
Step_2	Once the archive is downloaded to the platform, extract the archive content provided by Kontron 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/**	`[root@localhost ~]# cp -a /home/archive/. /boot/efi/`

Step_4	Verify that the **startup.nsh** script can be found directly in the **/boot/efi** directory.
	LocalServer_OSPrompt:~# **ls /boot/efi**
	NOTE: Some of the content of the archive could change depending on the version.
		`[root@localhost ~]# ls /boot/efi`
		`EFI`
		`firmware`
		`lan`
		`startup.nsh`

Step_5	Reboot the platform and access the UEFI/BIOS setup menu.	
Step_6	Navigate to the **Save & Exit** menu and then to the **Boot Override** section. Select the option that corresponds to the **UEFI: Built-in EFI Shell** and press **Enter** . The built-in EFI Shell should launch.	

		
Step_7	Press any key other than '**q**' to continue. The UEFI/BIOS upgrade should start.	
Step_8	Once completed, the BMC and the platform will automatically reset. It may take several seconds to complete the power cycle and the remote connection might be lost.	

Upgrading the UEFI/BIOS firmware from the server operating system

Prerequisites

1	The **.tar.gz** archive provided by Kontron has been downloaded 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

Procedure

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 the UEFI/BIOS firmware using the Web UI

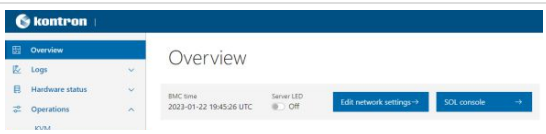
Prerequisites

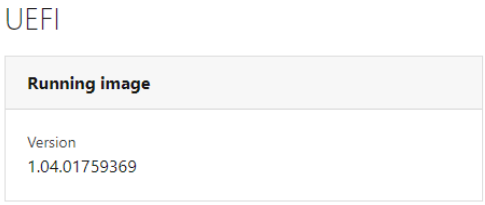
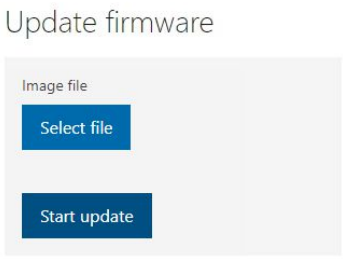
1	The web package (**.tar.gz**) provided by Kontron was downloaded on the remote computer.
2	Access to the BMC Web UI is required.

Relevant section:
Accessing a BMC using the Web UI

Procedure

	⚠ **Loss of user settings** ⚠ Using this UEFI/BIOS firmware upgrade method will revert all UEFI/BIOS settings to factory defaults. This includes device boot order and network boot parameters. Configuration changes may need to be reapplied and saved before the integrated server OS can boot.

Step_1	From the left-side menu of the BMC Web UI, click on **Operations** and then on **Firmware** .	

		
Step_2	Verify the current firmware version. Make sure that the new firmware is more recent.	
Step_3	From the **Update firmware** section, choose a **.tar.gz** file to upload for the UEFI/BIOS by clicking on **Select file** .	
Step_4	Click on **Start update** .	
Step_5	When the file has successfully been uploaded, a success message should appear in the top right corner.	
Step_6	Wait for the UEFI/BIOS to update. The page should refresh automatically upon successful update.	
Step_7	Once the UEFI/BIOS becomes available again, verify that the firmware version has changed.	

Upgrading the UEFI/BIOS firmware using Redfish

Prerequisites

1	The web package (**.tar.gz**) provided by Kontron was downloaded on the remote computer.
2	Access to the BMC Redfish interface is required.

Relevant sections:
Accessing a BMC using Redfish
Backing up the UEFI/BIOS

Procedure

	⚠ Loss of user settings ⚠ Using this UEFI/BIOS firmware upgrade method will revert all UEFI/BIOS settings to factory defaults. This includes device boot order and network boot parameters. Configuration changes may need to be reapplied and saved before the integrated server OS can boot.

Step_1	From the BMC Redfish interface, verify the current UEFI firmware version. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system | jq .BiosVersion**

	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.175.208/redfish/v1/Systems/system`
	`  | jq .BiosVersion`
	`"1.00.0968fc16"`

Step_2	(Optional) Update the current UEFI/BIOS firmware and configuration backup image. Please refer to the "Backup and restore" section for the procedure.
Step_3	Upload the firmware by executing the following command. The payload will be shutdown by the update service to be able to save the new firmware. RemoteComputer_OSPrompt:~$ **curl -k -s --request POST --url [ROOT_URL] /redfish/v1/UpdateService --header 'Content-Type: application/octet-stream' --upload-file ' [FILE_PATH]' | jq**

	`$ curl -k -s --request POST --url https://admin:ready2go@172.16.175.208/redfish/v1/UpdateService`
	`  --header 'Content-Type: application-/octet-stream' --upload-file 'ME1310-UEFI-1.06.096AF3C1-web`
	`.tar.gz' | jq`
	`{`
	`  "@odata.id": "/redfish/v1/TaskService/Tasks/1",`
	`  "@odata.type": "#Task.v1_4_3.Task",`
	`  "Id": "1",`
	`  "TaskState": "Running",`
	`  "TaskStatus": "OK"`
	`}`

Step_4	Note that the BMC is also rebooted during the new firmware activation and it can take a few minutes before the end of the firmware update and reboot process. When this is done, verify the version. RemoteComputer_OSPrompt:~$ **curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system | jq .BiosVersion**

	`$ curl -k -s --request GET --url https://admin:ready2go@172.16.175.208/redfish/v1/Systems/system`
	`  | jq .BiosVersion`
	`"1.06.096af3c1"`

Upgrading switch firmware

The network switch firmware can be upgraded using:

- SCP
- The switch NOS Web UI – This method can only be used if the Web connectivity is highly reliable. If the file transfer stops, simply start again.

Relevant section:
Network switch configuration load error messages (to troubleshoot error messages associated with an upgrade procedure)

	If error messages are generated when restoring the switch NOS configuration or upgrading its firmware, refer to the Troubleshooting section.

Upgrading the 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.
3	The NOS configuration has been backed up.

Relevant section:
Accessing the switch NOS

Procedure

	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]).

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**	NOSBBABA5BBABA5# firmware upgrade scp://user:password@192.168.0.10/KONTRON-NOS-2.26.016a3532. itb save-host-key Downloading... Got 18965810 bytes Starting flash update - do not power off device ! done
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:~# **show version** In the results, look for the version in the Primary Image section. In the image, the version is 2.26.016a3532.	NOSBBABA5BBABA5# show version *[...]* Primary Image ---------- Image : l inux (Active) Version : Kontron NOS IStaX 2.26.016a3532 Date : 2022-11-22T15:50:17-05:00 *[...]*

Upgrading the switch firmware using the switch NOS Web UI

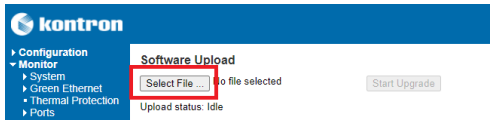
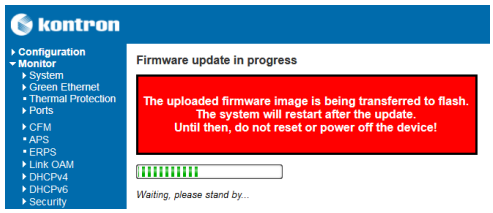
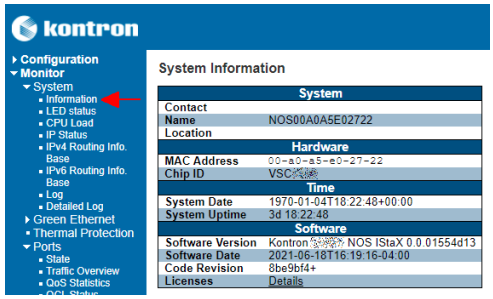
Prerequisites

1	Access to the switch NOS Web UI is required.
2	The . **itb** upgrade file provided by Kontron was downloaded on the remote computer.

Relevant section:
Accessing the switch NOS using the switch NOS Web UI

Procedure

If the procedure generates error messages, they will not be shown in the switch NOS Web UI. They are only visible from a CLI interface.

Step_1	From the left-side menu of the switch NOS Web UI, select **Maintenance** , **Software** and then **Upload** .	
Step_2	Click the **Select File** button and then choose the desired **.itb** file.	
Step_3	After selecting the file for the upgrade, click on **Start Upgrade** .	
Step_4	Wait for the upload and upgrade process to complete.	
Step_5	Once the upgrade is done, from the left-side menu, select **Monitor** , **System** and then **Information** . Confirm that the **Software Version** corresponds to that of the **.itb** file.	

Platform cooling and thermal management

Table of contents

Relevant sections:

Environmental considerations
Sensor list
Configuring sensors and thermal parameters

The ME1310 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 degrees Celsius

The system is designed to operate in a cold environment, but for all components to run in their specified temperature ranges, the system may need to be heated before startup. Heating elements are built-in for the integrated server processor and, optionally, for the PCIe add-in cards.

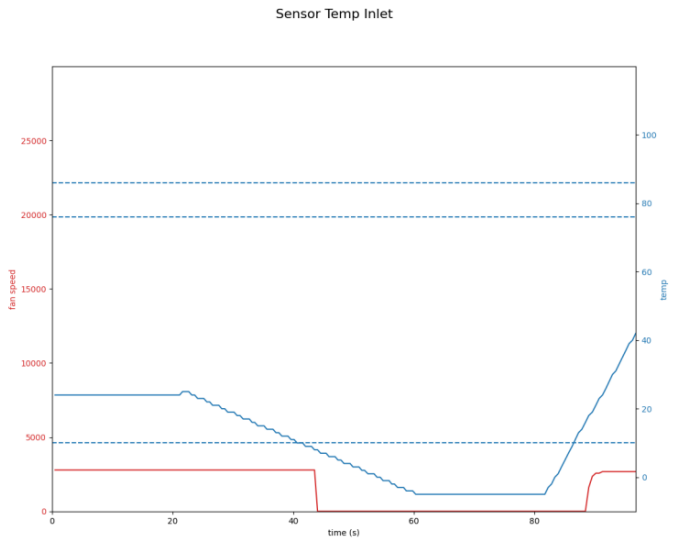
- When the platform is powered and designated components are detected at temperatures below their operating limits , an internal heating element preheats these components prior to the integrated server power on.
- Once the temperature of these components exceeds their lower operating limit, the integrated 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 degrees Celsius

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 30% 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 and M.2 module 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. Note that in a platform configured with

a pass-through IO module, the temperature of the SFP modules should be reported to the BMC by the customer application. The integrated Ethernet switch IO module autonomously reports the SFP module temperatures to the BMC.

Cooling management characteristics

- Minimum fan speeds are set to 30%.
- 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 ±15% for 30 seconds, the fan is marked as faulty and an event is registered. These events can be viewed only via Web UI or Redfish. The fan can later be restored if the speed comes back within the deviation range for a steady period of 5 seconds.
The platform fans are redundant. But when a fan is faulty, all fans will be set to maximum speed since the platform is operating in a degraded state.


```
{
    "@odata.context": "/redfish/v1/$metadata#LogEntry.LogEntry",
    "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries/#1614699759_4",
    "@odata.type": "#LogEntry.v1_4_0.LogEntry",
    "Created": "2021-03-02T15:42:39+00:00",
    "EntryType": "Event",
    "Id": "1614699759_4",
    "Message": "Fan_1 speed deviated.",
    "MessageArgs": [
        "Fan_1"
    ],
    "MessageId": "OpenBMC.0.1.FanSpeedDeviated",
    "Name": "System Event Log Entry",
    "Severity": "OK"
},
  {
      "@odata.context": "/redfish/v1/$metadata#LogEntry.LogEntry",
      "@odata.id": "/redfish/v1/Systems/system/LogServices/EventLog/Entries/#1614699764_4",
      "@odata.type": "#LogEntry.v1_4_0.LogEntry",
      "Created": "2021-03-02T15:42:44+00:00",
      "EntryType": "Event",
      "Id": "1614699764_4",
      "Message": "Fan_1 speed restored.",
      "MessageArgs": [
          "Fan_1"
      ],
      "MessageId": "OpenBMC.0.1.FanSpeedRestored",
      "Name": "System Event Log Entry",
      "Severity": "OK"
  },
```


To access the SEL using Redfish to see the events, refer to System event log .

Default temperature thresholds

To see temperature thresholds, refer to the instruc tions provide d in Monitoring sensors and Configuring sensors and thermal parameters .

Troubleshooting

Collecting diagnostics

Table of contents

The following information could be required when contacting the support team to make the proper board health diagnostics.
However, if the platform is inoperable, the some of the information can be retrieved using a QR code .

Collecting the system inventory

The following information could be used in order to make the proper board health diagnostics. Refer to System inventory .

- FRU information
- BMC, UEFI, FPGA firmware version
- Power supply type
- Product IO module information
- Processor device information
- Memory device configuration
- Storage devices
- UEFI/BIOS configuration
- Ethernet switch running configuration
- Ethernet switch versions

Collecting the event logs

Multiple event logs could be used in order to make the proper board health diagnostics .

- BMC event logs. Refer to BMC system event log .
- Switch NOS event log. Refer to NOS system event log .
- UEFI/BIOS POST codes (optional). Refer to POST code logs .

Creating and collecting the BMC Debug Collector dumps

Relevant section:
Accessing a BMC using Redfish

The platform BMC can create state log dumps. Creation of such dumps may be triggered autonomously by internal triggers and remotely.

Remotely triggering the creation of a BMC state log dump using Redfish

Step_1	RemoteComputer_OSPrompt:~$ curl -k -s --request POST --url [ROOT_URL]/redfish/v1/Managers/bmc/LogServices/Dump/Actions/LogService.CollectDiagnosticData --data '{"DiagnosticDataType": "Manager"}'

```
$ curl -k -s --request POST --url https://admin:ready2go@192.168.8.78/redfish/v1/Managers/bmc/LogServices/Dump/Actions/LogService.CollectDiagnosticData --data '{"DiagnosticDataType": "Manager"}' | jq .
{
  "@odata.id": "/redfish/v1/TaskService/Tasks/0",
  "@odata.type": "#Task.v1_4_3.Task",
  "Id": "0",
  "TaskState": "Running",
  "TaskStatus": "OK"
}
```

Step_2	(Optional) Monitor the task returned in the log creation command above to guide retrieval of the dump by confirming the BMC has finished the task. Also, the entry ID is part of the final response. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/TaskService/Tasks/0" | jq .

```
$ curl -k -s --request GET --url https://admin:ready2go@192.168.8.78"/redfish/v1/TaskService/Tasks/0" | jq .
{
  "@odata.id": "/redfish/v1/TaskService/Tasks/0",
  "@odata.type": "#Task.v1_4_3.Task",
  "EndTime": "2023-12-06T21:01:41+00:00",
  "Id": "0",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_0.Message",
      "Message": "The task with id 0 has started.",
      "MessageArgs": [
        "0"
      ],
      "MessageId": "TaskEvent.1.0.1.TaskStarted",
      "Resolution": "None.",
      "Severity": "OK"
    },
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "Message": "Successfully Completed Request",
      "MessageArgs": [],
      "MessageId": "Base.1.8.1.Success",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ],
  "Name": "Task 0",
  "Payload": {
    "HttpHeaders": [
      "Host: 192.168.8.78",
      "User-Agent: curl/8.4.0",
      "Accept: */*",
      "Content-Length: 33",
      "Location: /redfish/v1/Managers/bmc/LogServices/Dump/Entries/60"
    ],
    "HttpOperation": "POST",
    "JsonBody": "{\n  \"DiagnosticDataType\": \"Manager\"\n}",
    "TargetUri": "/redfish/v1/Managers/bmc/LogServices/Dump/Actions/LogService.CollectDiagnosticData"
  },
  "PercentComplete": 0,
  "StartTime": "2023-12-06T21:00:30+00:00",
  "TaskMonitor": "/redfish/v1/TaskService/Tasks/0/Monitor",
  "TaskState": "Completed",
  "TaskStatus": "OK"
}
```

Listing available BMC state log dump entries using Redfish

Step_1	List all dumps stored by the BMC. RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc/LogServices/Dump/Entries

```
$ curl -k -s --request GET --url https://admin:ready2go@192.168.8.78/redfish/v1/Managers/bmc/LogServices/Dump/Entries | jq .
{
  "@odata.id": "/redfish/v1/Managers/bmc/LogServices/Dump/Entries",
  "@odata.type": "#LogEntryCollection.LogEntryCollection",
  "Description": "Collection of BMC Dump Entries",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Managers/bmc/LogServices/Dump/Entries/58",
      "@odata.type": "#LogEntry.v1_7_0.LogEntry",
      "AdditionalDataSizeBytes": 6464,
      "AdditionalDataURI": "/redfish/v1/Managers/bmc/LogServices/Dump/Entries/58/attachment",
      "Created": "2023-12-05T20:42:48+00:00",
      "DiagnosticDataType": "Manager",
      "EntryType": "Event",
      "Id": "58",
      "Name": "BMC Dump Entry"
    },
    {
      "@odata.id": "/redfish/v1/Managers/bmc/LogServices/Dump/Entries/59",
      "@odata.type": "#LogEntry.v1_7_0.LogEntry",
      "AdditionalDataSizeBytes": 6408,
      "AdditionalDataURI": "/redfish/v1/Managers/bmc/LogServices/Dump/Entries/59/attachment",
      "Created": "2023-12-05T20:57:57+00:00",
      "DiagnosticDataType": "Manager",
      "EntryType": "Event",
      "Id": "59",
      "Name": "BMC Dump Entry"
    }
  ],
  "Members@odata.count": 2,
  "Name": "BMC Dump Entries"
}
```

Retrieving a BMC state log dump entry using Redfish

Step_1	Download the desired BMC LogService dump by specifying the entry number [DUMP_ID] . RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc/LogServices/Dump/Entries/ [DUMP_ID] /attachment --output [OUTPUT_FILE.TAR.XZ]

	`$ curl -k -s --request GET --url https://admin:ready2go@192.168.8.78/redfish/v1/Managers/bmc/LogServices/Dump/Entries/59/attachment --output BMC_diag_dump_id59.tar.xz`
	
	`$ ls`
	`BMC_diag_dump_id59.tar.xz`

Step_2	Extract the .xz compressed archive. RemoteComputer_OSPrompt:~$ tar -Jxf [OUTPUT_FILE.TAR.XZ]

	`$ tar -Jxvf BMC_diag_dump.tar.xz`
	`obmcdump_59_1701809877/`
	`obmcdump_59_1701809877/host-state.log`
	`obmcdump_59_1701809877/hostnamectl.log`
	`obmcdump_59_1701809877/chassis-state.log`
	`obmcdump_59_1701809877/bmc-state.log`
	`obmcdump_59_1701809877/uptime.log`
	`obmcdump_59_1701809877/cpuinfo`
	`obmcdump_59_1701809877/elog-64.log`
	`obmcdump_59_1701809877/os-release`
	`obmcdump_59_1701809877/journal-pid-619.log`
	`obmcdump_59_1701809877/top.log`
	`obmcdump_59_1701809877/meminfo`
	`obmcdump_59_1701809877/failed-services.log`
	`obmcdump_59_1701809877/dreport.log`
	`obmcdump_59_1701809877/disk-usage.log`
	`obmcdump_59_1701809877/summary.log`

Deleting a BMC state log dump entry using Redfish

Step_1	Delete a specific dump. RemoteComputer_OSPrompt:~$ curl -k -s --request DELETE --url [ROOT_URL]/redfish/v1/Managers/bmc/LogServices/Dump/Entries/ [DUMP_ID]

	`$ curl -k -s --request DELETE --url https://admin:ready2go@192.168.8.78/redfish/v1/Managers/bmc/LogServices/Dump/Entries/59 | jq`
	
	`$`

Clearing all BMC state log dump entries using Redfish

Step_1	Delete all the dumps. RemoteComputer_OSPrompt:~$ curl -k -s --request POST --url [ROOT_URL]/redfish/v1/Managers/bmc/LogServices/Dump/Actions/LogService.ClearLog

	`$ curl -k -s --request POST --url https://admin:ready2go@192.168.8.78/redfish/v1/Managers/bmc/LogServices/Dump/Actions/LogService.ClearLog | jq .`
	
	`$`

Collecting system information using a QR code

Relevant section:
MAC addresses

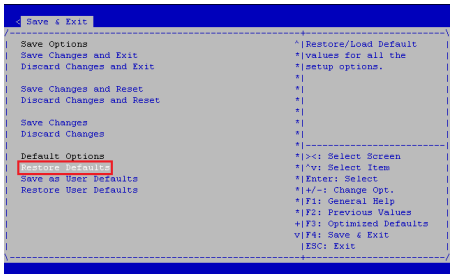
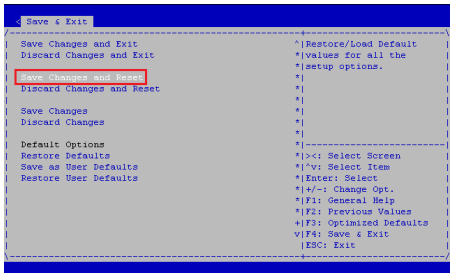
Step_1	Using a QR code application, scan the QR code of the platform. Record the information obtained in your device (e.g. by taking a screen shot). S/N:9017020001 = Platform serial number P/N:1065-2823 = Platform part number BATCH:0A00000001 = Platform production lot number MAC: 00A0A5D6402A = First MAC address attributed to the BMC/server. Value to be used to replace MAC_BASE. 00A0A5E1B934 = First MAC address attributed to the integrated Ethernet switch. Value to be used to replace SW_MAC_BASE. This is only present for a platform configured with the IO Ethernet switch module.	S/N:9017020001 P/N:1065-2823 BATCH:0A00000001 MAC: 00A0A5D6402A 00A0A5E1B934

Factory default

Table of contents

Restoring default UEFI/BIOS settings

Refer to Accessing the UEFI or BIOS for access instructions.

Step_1	From the UEFI/BIOS setup menu, navigate to the **Save & Exit** menu and select **Restore Defaults** .	
Step_2	Select **Save Changes and Reset** .	
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. Your access to system components could be interrupted because of changes to various elements, including:

- NOS access via network IP addresses
- NOS user configuration
- Other system components, due to switch forwarding configurations (e.g., VLAN)

Refer to Description of system access methods to select an appropriate path to access the platform components.
It is also **recommended to back up the startup configuration before restoring the default settings** . The backed up file could serve as a reference for future configuration.

Changes to the switch NOS configuration are not persistent after rebooting the switch NOS.
To preserve configurations, the current configuration needs to be saved to startup-config.
From the switch NOS Web UI:

- Select **Maintenance** , **Configuration** and then **Save startup-config** . Click on **Save Configuration** to confirm the change.

From the switch NOS CLI:

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

Relevant sections:
Description of system access methods
Backup and restore

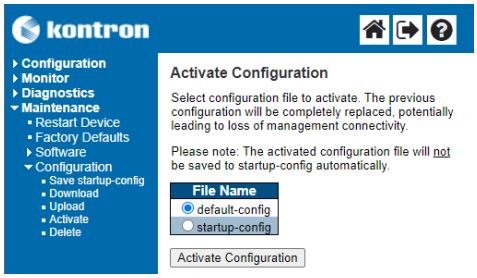
Restoring default switch NOS settings using the CLI

Refer to Accessing the switch NOS for access instructions.

Step_1	Restore the default configuration. LocalSwitchNOS_OSPrompt:~# **reload defaults**	`# reload defaults` `% Reloading defaults. Please stand by.`
Step_2	(Optional) To make the change persistent, save running-config to startup-config.	

Restoring default switch NOS settings using the Web UI

Refer to Accessing the switch NOS for access instructions.

Step_1	From the left-side menu, select **Maintenance, Configuration** and then **Activate** .	
Step_2	Click on the **default-config** radio button.	
Step_3	Press on the **Activate Configuration** button to confirm.	
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 Accessing a BMC using IPMI (KCS) method.

Step_1	Identify the **ID** of the user with the password to restore.
	LocalServer_OSPrompt:~# **ipmitool user list [CHANNEL]**
		`# ipmitool user list 1`
		`ID  Name  Callin  Link Auth  IPMI Msg  Channel Priv Limit`
		`1  admin  false  true  true  ADMINISTRATOR`
		`2  mynewuser  false  true  true  ADMINISTRATOR`
		`3  true  false  false  NO ACCESS`
		`4  true  false  false  NO ACCESS`

Step_2	Reset the password. LocalServer_OSPrompt:~# **ipmitool user set password [USER_ID] [NEW_PASSWORD]**	`# ipmitool user set password 1 "newpassword123456"`

Network switch configuration load error messages

This section describes how to proceed if error messages are generated when:

- The NOS firmware is upgraded. In rare instances, configuration commands may change format in a new firmware version and therefore need correcting.
- The NOS configuration is restored or uploaded using configuration commands that have changed format or was modified remotely with errors.

NOTE: Configuration load errors may only be printed on the serial console interface of the switch NOS.

Relevant section:
Backup and restore (to have a reference of the startup configuration)

Access the switch NOS CLI. Refer to Accessing the switch network operating system for access instructions.

Step_1	Back up the startup configuration to have a reference.	
Step_2	Restore factory default values. LocalSwitchNOS_OSPrompt:~# **reload defaults**	NOS00A1A5E01C4F# reload defaults % Reloading defaults. Please stand by.
Step_3	Using the reference startup configuration, manually enter the configuration items that differ from the original configuration, and correct errors if needed.	
Step_4	Make the change persistent by saving the running-config to startup-config. LocalSwitchNOS_OSPrompt:~# **copy running-config startup-config**	NOS00A1A5E01C4F# copy running-config startup-config Building configuration... % Saving 1859 bytes to flash:startup-config
Step_5	Reboot the NOS to make sure the configuration was applied correctly. LocalSwitchNOS_OSPrompt:~# **reload cold**	

Support information

To ensure a timely treatment of your support request, Kontron recommends collecting the system inventory and the relevant diagnostics .
Kontron's technical support team can be reached through the following means:

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

For sales information, including current and future product options, please contact Kontron Sales Support in Canada through the following means:

- By phone: 1-800-387-4222
- By email: gss-com@kontron.com

Knowledge base

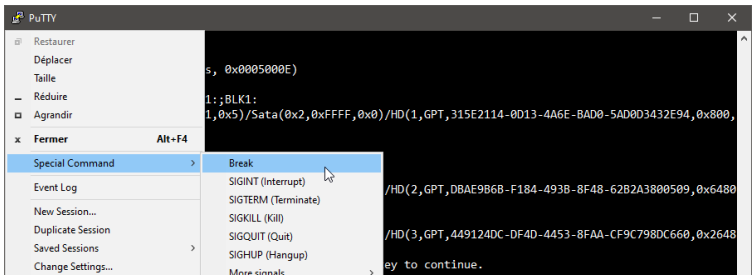
Sending a BREAK signal over a serial connection

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                    |
...
| send break.........F                    |
```

Picocom

A **BREAK** signal can be sent from the picocom Linux utility's help.

```
*** Picocom commands (all prefixed by [C-a])
...
*** [C-|] : Send break
```

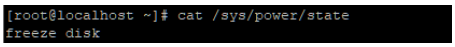
Serial console servers

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.

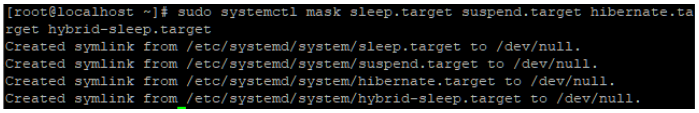
Disabling sleep states in Linux

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 Accessing the operating system of a server for access instructions.

Verifying enabled sleep states

Step_1	Verify enabled sleep states. LocalServer_OSPrompt:~# **cat /sys/power/state**	

Disabling sleep states

Step_1	Disable sleep states using systemd. LocalServer_OSPrompt:~# **sudo systemctl mask sleep.target suspend.target hibernate.target hybrid-sleep.target**	

Application notes

Generating custom secure boot keys

Relevant section:
Provisioning custom secure boot keys

To provision custom secure boot keys, keys may have to be generated. This article provides an example using CentOS 7.

Prerequisites

1	Packages efitools and sbsigntools must be available. These packages are not official CentOS packages.

Procedure

Step_1	Run the following commands on the system you need to generate keys for. mkdir make_keys cd make_keys wget https://github.com/freshautomations/efitools-centos/releases/download/2019-05-12/efitools-v1.9.2-1.x86_64.rpm wget https://github.com/freshautomations/efitools-centos/releases/download/2019-05-12/sbsigntools-v0.9.2-1.x86_64.rpm wget https://www.rodsbooks.com/efi-bootloaders/mkkeys.sh chmod +x mkkeys.sh yum install sbsigntools-v0.9.2-1.x86_64.rpm efitools-v1.9.2-1.x86_64.rpm ./mkkeys.sh
Step_2	The commands will generate a lot of files. You need the *.cer file to use in the provisioning procedure.

Provisioning custom secure boot keys

Table of contents

Introduction

This article describes how to provision a custom set of Secure Variables used as part of the Secure Boot feature.
Secure Boot is a UEFI-defined feature used to authenticate a UEFI executable, such as an OS loader, using digital signing mechanisms based on the Public Key Infrastructure process, reducing the risks of pre-boot malware attacks. The feature uses a database of authorized signatures to confirm the UEFI executable integrity prior to execution.
Boards will typically have a pre-loaded set of Platform Key (PK), Key Exchange Keys (KEK), authorized signature database (db) and blacklisted / revoked signature database (dbx) as defined by the OEM, as well as some industry-standard certificates issued by Microsoft that allow booting Windows or well-known Linux distributions such as Ubuntu. It may be desirable for an end customer to update these keys with their own set for security reasons.
This document assumes the reader has some knowledge about the Secure Boot process, and that the required set of keys and certificates has been properly generated. The following link provides guidelines on creating and managing such keys and certificates:
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-secure-boot-key-creation-and-management-guidance

Updating secure boot keys from the UEFI setup utility

Prerequisites

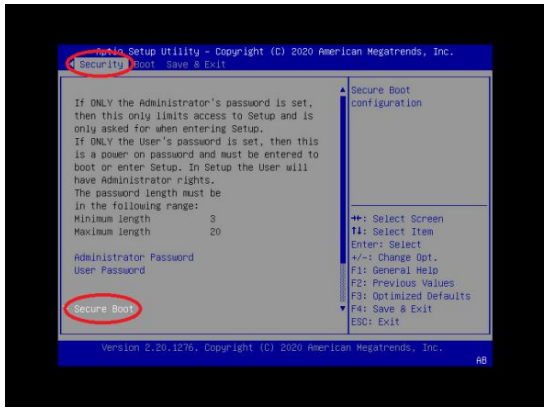
1	A set of Secure Boot keys has been created (PK, KEK and db).
2	Public Key certificates that are to be provisioned are in DER format.
3	Public Key certificates are present on a FAT-partitioned USB drive, which is connected to the board. If Virtual Media redirection is available, it is also possible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

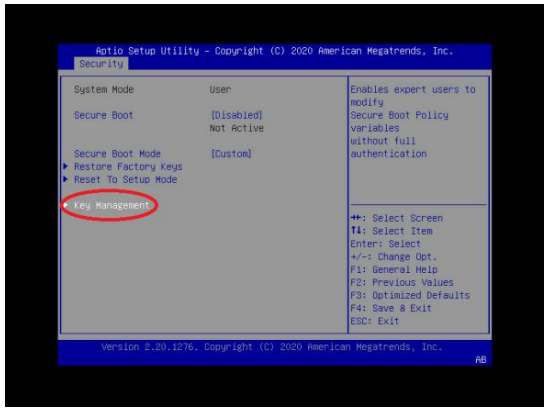
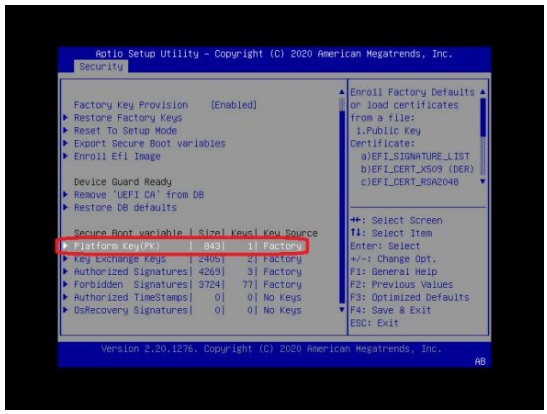
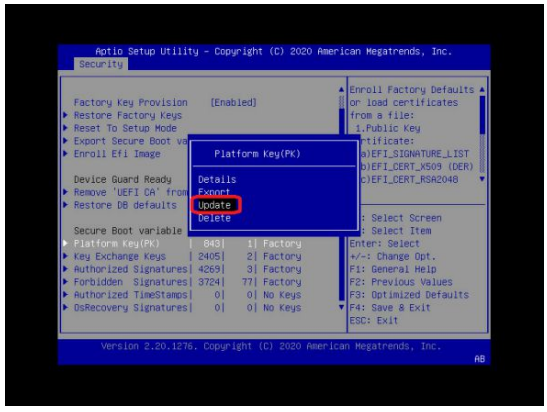
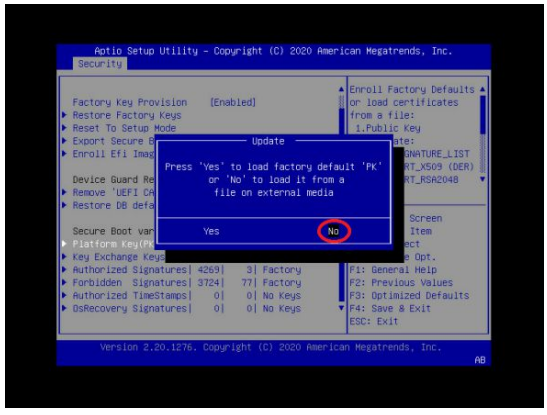
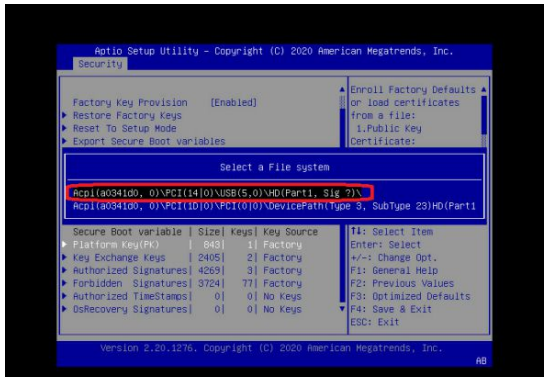
Relevant section:
Generating custom secure boot keys

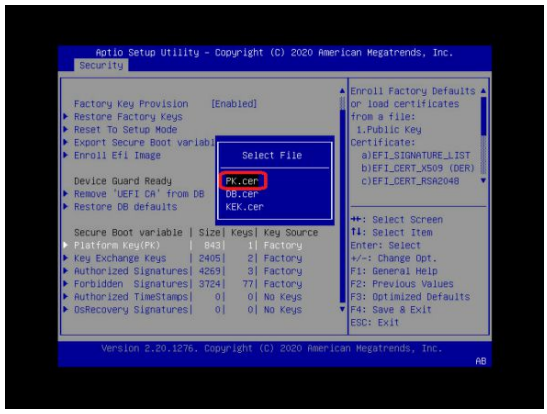
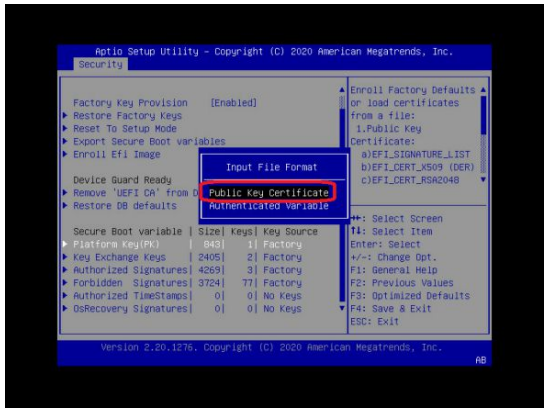
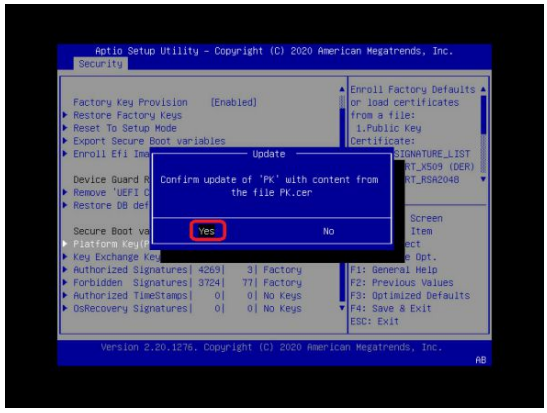
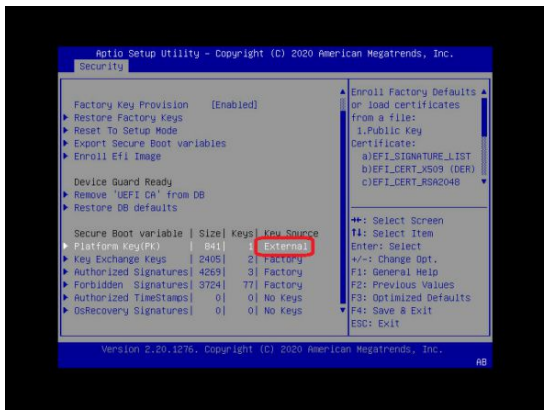
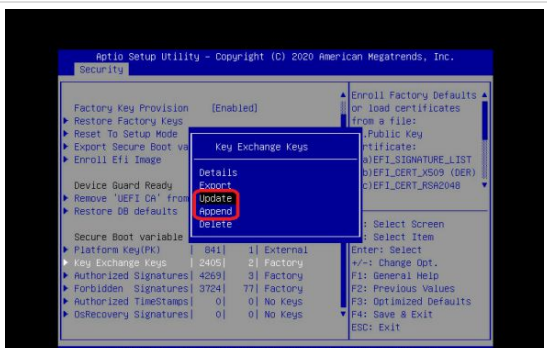
i	As the current time is verified against certificate timestamps as a security measure, make sure the system time is valid prior to manipulating Secure Boot variables. Otherwise, a Security Violation error will be obtained and no change will be possible.

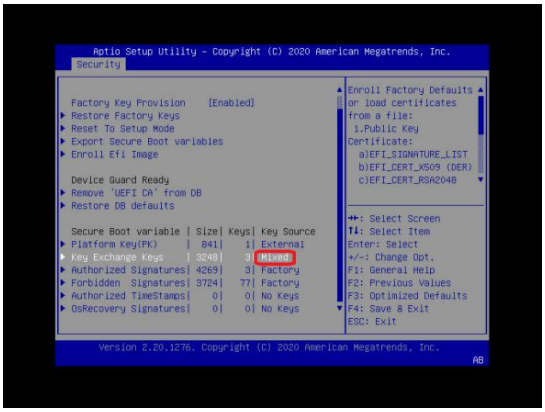
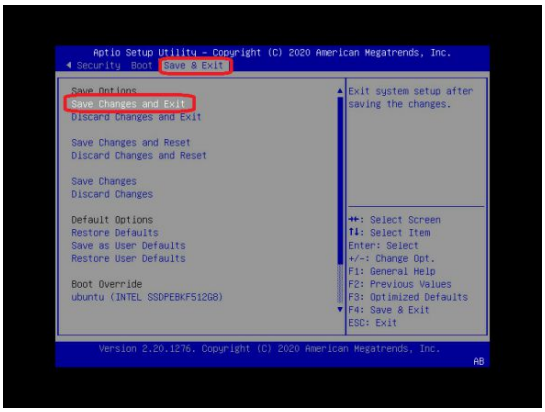
Procedure

Refer to Accessing the UEFI or BIOS for access instructions.

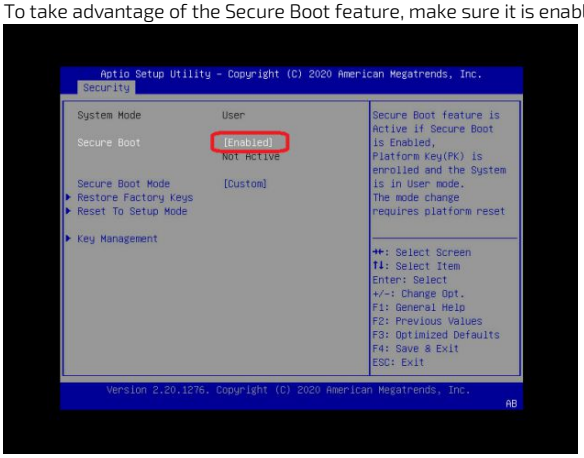
Step_1	Access the UEFI Setup Utility by pressing F2 or DEL when the sign-on screen is displayed during boot.	
Step_2	Access the **Secure Boot** submenu from the **Security** tab.	

Step_3	Access the Key Management page by selecting the **Key Management** menu item.	
Step_4	Default Factory Keys should already be provisioned, as identified by the "Factory" attribute in the Key Source column in the Secure Boot variable table. To replace the default Platform Key with your own, select **Platform Key(PK)** .	
Step_5	Select **Update** from the pop-up window.	
Step_6	Select **No** to load a key from an external media.	
Step_7	A list of available file systems will be displayed, using their corresponding UEFI device path. Select the USB device where the Public Key certificates are located. Note that if Virtual Media redirection is used, the device will be identified as a CDROM.	

Step_8	From the list of files, select the Public Certificate file for the Platform Key (PK.cer in this example).	
Step_9	Specify that the file format is **Public Key Certificate** .	
Step_10	Select **Yes** to confirm Platform Key update.	
Step_11	Confirm that the update completed successfully. The table should now show that a key was added from an "External" Key Source.	
Step_12	Select **Key Exchange Keys** to update or append the KEK database with your own. In this case: • Selecting **Update** from the pop-up window will erase the pre-provisioned KEK entries and add a new KEK as a single entry; • Selecting **Append** will add the new KEK to the database.	

		
Step_13	Follow steps 4 to 11 to add a new KEK entry. If the KEK was appended to the database, the Key Source will be "Mixed".	
Step_14	Select **Authorized Signatures** to add an authorized Public Key certificate to the db. As for KEK: • Selecting **Update** from the pop-up window will erase the pre-provisioned db entries and add a new certificate as a single entry; • Selecting **Append** will add the new certificate to the database. Follow steps 4 to 11 to add a new db entry. If the certificate was appended to the database, the Key Source will be "Mixed".	
Step_15	Select **Save Changes and Exit** from the Setup Utility.	

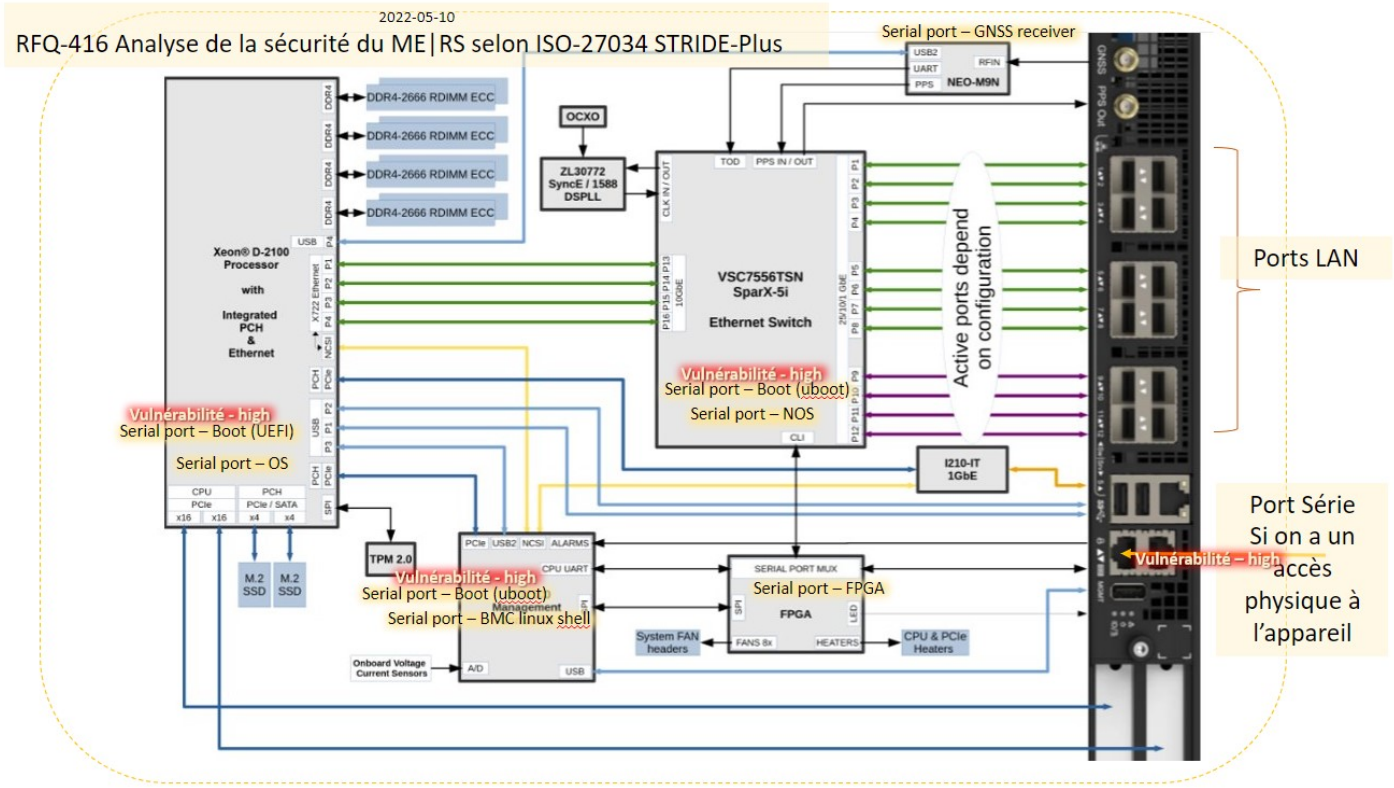
To take advantage of the Secure Boot feature, make sure it is enabled in the Security → Secure Boot submenu.



Security for External Interfaces

Introduction

This documents provides security recommendations for external interfaces of ME and RS systems.
Securing the interfaces of the system and understanding how critical these interfaces are in a security standpoint is an important step before deploying the ME and RS systems.
The information provided take advantage of the User Manual for the step by step instructions.
As a reference you will see in the image below an extract of the Security Analysis process performed on the ME and RS system.



External interfaces

Physical Interface	ISO-27034 ME|RS Physical Interfaces Analysis :: Security Recommendations
Serial Port ISO-27034-ME|RS-Interfaces-Security-Info1	ME-RS1310 serial port provides access to many subcomponents of the system: Host CPU, BMC Linux console, NOS console of Ethernet Switch, GNSS Receiver and FPGA. Various configurations and controls could be done using serial access of each of these subcomponents. Therefore, in a security standpoint it is required to protect and limit physical access to the system to prevent unintended action(s) from an unauthorized user.
Ethernet Switch Ports ISO-27034-ME|RS-Interfaces-Security-Info2 **SFP Ports** ISO-27034-ME|RS-Interfaces-Security-Info3	In order to reduce the possibility of unauthorized access to the system, it is good practice to disable all unused Ethernet switch ports. Here the reference information on how to disable SFP in Ethernet Switch configuration https://kontron.atlassian.net/wiki/spaces/ME1310/pages/3245606637/Configuring+the+switch#Configuringtheswitch-Disablingaswitchport Search for 'Disabling a switch port' into the user manual. VLAN could also be used to further limit access to the Ethernet switch configuration. In particular one could be interested to restrict Ethernet switch configuration access from external user connected to the front haul LAN ports. More information could be provided on request.
Ethernet Switch ISO-27034-ME|RS-Interfaces-Security-Info4	It is recommended to change the Ethernet Switch password. Default user names and passwords https://kontron.atlassian.net/wiki/spaces/ME1310/pages/3245608154/Configuring+and+managing+users Configuring and managing switch NOS users Into the user manual search for 'Default user name and password' 'Configuring and managing users' 'Configuring and managing switch NOS users'
BMC ISO-27034-ME|RS-Interfaces-Security-Info5 **Serial Over LAN (SOL)** ISO-27034-ME|RS-Interfaces-Security-Info7 **KVM** ISO-27034-ME|RS-Interfaces-Security-Info8	It is recommended to change the BMC, SOL and KVM password. You can change the password from WEB, RedFish or IPMI interfaces of BMC. Changing it at one place change it for all BMC interfaces. Configuring and managing BMC users Default user names and passwords Accessing the operating system of a server Accessing the UEFI or BIOS Accessing the switch NOS Into the user manual search for 'Configuring and managing BMC users ' 'Default user names and passwords ' 'Accessing an OS using Serial over SSH ' 'Accessing an OS using IPMI Serial over LAN ' 'Accessing the UEFI or BIOS using Serial over SSH ' 'Accessing the switch NOS CLI using BMC Web UI Serial over LAN console '
OS Boot ISO-27034-ME|RS-Interfaces-Security-Info6	It is recommended to enable Secure Boot to protect Operating System (OS) integrity. [Content under creation] https://kontron.atlassian.net/wiki/spaces/ME1310/pages/3245607973/Configuring+UEFI+BIOS+options#ConfiguringUEFI%2FBIOSoptions-Changingthebootorder Into the user manual search for 'Enabling Secure Boot' It is also recommended to change the password of the UEFI [Content under creation] WIP - Configuring and managing UEFI/BIOS users Into the user manual search for 'Configuring and managing UEFI/BIOS users'
Boot from USB ISO-27034-ME|RS-Interfaces-Security-Info9 **Upgrade Firmware via USB** ISO-27034-ME|RS-Interfaces-Security-Info10	It is recommended to disable USB ports. If an unauthorized person has a physical access to the system, then if USB ports are disabled it will prevent accessing, booting or upgrading the system via this interface. [Content under creation] https://kontron.atlassian.net/wiki/spaces/ME1310/pages/3245607973/Configuring+UEFI+BIOS+options#ConfiguringUEFI%2FBIOSoptions-DisablingUSBports Into the user manual search for 'Disabling USB ports'

Reference guides

Supported Redfish commands

Table of contents

The information is presented in the following format:

- Description | URL | Type

Schema definition

Schema definition for a specific type can be retrieve from https://redfish.dmtf.org

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
- Collection of thermal sensors | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Thermal | Thermal.v1_4_0

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
- Collection of current event subscriptions | /redfish/v1/EventService/Subscriptions | EventDestinationCollection

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

Application commands

IPM device commands

Net function	Command	Command name	Supported / Unsupported
0x06	0x01	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	0x07	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
0x06	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
0x06	0x0D	Get Configurable Command Sub-functions	Unsupported
0x06	0x62	Set Command Sub-function Enables	Unsupported
0x06	0x63	Get Command Sub-function Enables	Unsupported
0x06	0x52	Master Write-Read	Unsupported

* Commands are not rejected and can cause unpredictable behavior.
**This command is mandatory in IPMI spec, so has been implemented ONLY to return one of the defined return code for this command: 0x56 = "Self Test function not implemented in this controller".

Watchdog timer commands

Net function	Command	Command name	Supported / Unsupported
0x06	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
0x06	0x2E	Set BMC Global Enables	Supported
0x06	0x2F	Get BMC Global Enables	Supported
0x06	0x30	Clear Message Flags	Supported
0x06	0x31	Get Message Flags	Supported
0x06	0x32	Enable Message Channel Receive	Unsupported
0x06	0x33	Get Message	Supported
0x06	0x34	Send Message	Supported
0x06	0x35	Read Event Message Buffer	Supported
0x06	0x36	Get BT Interface Capabilities	Supported
0x06	0x37	Get System GUID	Supported
0x06	0x38	Get Channel Authentication Capabilities	Supported
0x06	0x39	Get Session Challenge	Unsupported
0x06	0x3A	Activate Session	Unsupported
0x06	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
0x06	0x49	Deactivate Payload	Supported
0x06	0x4A	Get Payload Activation Status	Supported
0x06	0x4B	Get Payload Instance Info	Supported
0x06	0x4C	Set User Payload Access	Supported
0x06	0x4D	Get User Payload Access	Supported
0x06	0x4E	Get Channel Payload Support	Supported
0x06	0x4F	Get Channel Payload Version	Supported
0x06	0x50	Get Channel OEM Payload Info	Unsupported
0x06	0x54	Get Channel Cipher Suites	Supported
0x06	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
0x00	0x00	Get Chassis Capabilities	Supported
0x00	0x01	Get Chassis Status	Supported
0x00	0x02	Chassis Control	Supported
0x00	0x04	Chassis Identify	Supported
0x00	0x05	Set Chassis Capabilities	Supported
0x00	0x06	Set Power Restore Policy	Supported
0x00	0x07	Get System Restart Cause	Unsupported*
0x00	0x08	Set System Boot Options	Supported
0x00	0x09	Get System Boot Options	Supported
0x00	0x0A	Set Front Panel Button Enables	Unsupported*
0x00	0x0B	Set Power Cycle Interval	Unsupported
0x00	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	0x00	Get Bridge State	Unsupported
0x02	0x01	Set Bridge State	Unsupported
0x02	0x02	Get ICMB Address	Unsupported
0x02	0x03	Set ICMB Address	Unsupported
0x02	0x04	Set Bridge Proxy Address	Unsupported
0x02	0x05	Get Bridge Statistics	Unsupported
0x02	0x06	Get ICMB Capabilities	Unsupported
0x02	0x08	Clear Bridge Statistics	Unsupported
0x02	0x09	Get Bridge Proxy Address	Unsupported
0x02	0x0A	Get ICMB Connector Info	Unsupported

Bridge discovery commands

Net function	Command	Command name	Supported / Unsupported
0x02	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
0x04	0x26	Set Sensor Threshold	Supported
0x04	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	0x10	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
0x0c	0x01	Set LAN Configuration Parameters	Supported
0x0c	0x02	Get LAN Configuration Parameters	Supported
0x0c	0x03	Suspend BMC ARPs	Unsupported

Serial over LAN commands

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

Kontron OEM commands

Net function	Command	Command name	Supported / Unsupported
0x3C	0x07	UEFI Recovery	Supported

Document symbols and acronyms

Symbols

The following symbols are used in Kontron documentation.

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

Electric Shock!
This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of them. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.
Please also refer to the "High-Voltage Safety Instructions" portion below in this section.

ESD Sensitive Device!
This symbol and title inform that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.

HOT Surface!
Do NOT touch! Allow to cool before servicing.

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

This symbol precedes helpful hints and tips for daily use.

Acronyms

ACPI	Advanced Configuration and Power Interface
AI	Artificial Intelligence
AIC	Add-in Card (e.g. PCI Express)
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BIOS	Basic Input/Output System
BMC	Baseboard Management Controller
BSP	Board Support Package
CBIT	Continuous Built-In Test
CE	Community European (EU mark)
CLI	Command-Line Interface
COMe	COM-express
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

EEPROM	Electrically Erasable Programmable Read-Only Memory
EFI	Extensible Firmware Interface
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ETSI	European Telecommunications Standards Institute
ETSI	European Telecommunications Standards Institute
eUSB	Embedded Universal Serial Bus
FCC	Federal Communications Commission
FH/FL	Full Height/Full Length
FPGA	Field Programmable Gate Array
FRAU	Field Replaceable Unit
FRU	Field Replaceable Unit
Gb, Gbit	Gigabit
GB, Gbyte	Gigabyte – 1024 MB
GbE	Gigabit Ethernet
GND	Ground
GPI	General Purpose Input
GPIO	General Purpose Input/Output
GPO	General Purpose Output
GPS	Global Positioning System
GPU	Graphics Processing Unit
GUI	Graphical User Interface
HDD	Hard Disk Drive
Hz	Hertz – 1 cycle/second
I/O	Input/Output
I^2C	Inter-Integrated Circuit Bus
iBMC	Integrated Baseboard Management Controller
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMU	Inertial Measurement Unit
IOL	IPMI over LAN
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IRQ	Interrupt Request Line
KB, Kbyte	Kilobyte – 1024 bytes
KCS	Keyboard Controller Style
KEAPI	Kontron Embedded Application Programming Interface
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LED	Light-Emitting Diode
LP	Low Profile
LPC	Low Pin Count
LVDS	Low Voltage Differential SCSI
MAT	Maximum Ambient Temperature
MB, Mbyte	Megabyte – 1024 KB
MCU	Microcontroller Unit
MEC	Multi-Access Edge Computing
MXM	Mobile PCI Express Module

NCSI	Network Communications Services Interface
NEBS	Network Equipment-Building System
NIC	Network Interface Card, or Network Interface Controller, or Network Interface Controller port
NMI	Non-Maskable interrupt
NOS	Network Operating System
NVMe	Non-Volatile Memory Express
OCXO	Oven-Controlled Crystal Oscillator
OS	Operating System
OTP	Over-Temperature Protection
OVP	Over-Voltage Protection
PBIT	Power On Built-In Test
PCH	Platform Controller Hub
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PECI	Platform Environment Control Interface
PIRQ	PCI Interrupt Request Line
PMbus	Power Management Bus
PMM	POST Memory Manager
PnP	Plug and Play
POC	Proof of Concept
POST	Power-On Self Test
PSU	Power Supply Unit
PTP	Precision Time Protocol
PXE	Preboot eXecution Environment
QM	Quality Managed
RAID	Redundant Array of Independent Disks
RAN	Radio Access Network
RAS	Reliability, Availability, and Serviceability
RDIMM	Registered Dual In-Line Memory Module
RDP	Remote Desktop
RMM	Remote Management Module
RoHS	Restriction of Hazardous Substances
SAS	Serial Attached SCSI (Small Computer System Interface)
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer Systems Interface
SDRAM	Synchronous Dynamic RAM
SEL	System Event Log
SFP+	Small Form-factor Pluggable that supports data rates up to 10.0 Gbps
SMBus	System Management Bus
SMS	Server Management Software
SNMP	Simple Network Management Protocol
SOC	System on a Chip
SOL	Serial over LAN
SSD	Solid State Drive
SSH	Secure Shell
THOL	Tested Hardware and Operating System List
TPM	Trusted Platform Module
TUV	Technischer Uberwachungs-Verein (A safety testing laboratory with headquarters in Germany)

TÜV	Technischer Überwachungs-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
VPD	Vital Product Data
vRAN	Virtualized Radio Access Network
VSB	Voltage Standby
W	Watt
WEEE	Waste Electrical and Electronic Equipment
Ω	Ohm