Backup and restore
Upgrading
Platform cooling and thermal management
Troubleshooting
Collecting diagnostics
Factory default
Support information
Knowledge base
Sending a BREAK signal over a serial connection
Disabling sleep states in Linux
Application notes
Generating custom secure boot keys
Provisioning custom secure boot keys
Reference guides
Supported Redfish commands
Supported IPMI commands
Document symbols and acronyms
Product description

Table of contents

- ME1310 flexible edge server for rapid deployment of telecom and 5G services
  - Main applications
  - Main features

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

The Kontron ME1310 high performance 1U edge server is a distributed 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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Brief description of changes</th>
<th>Date of issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>First client release</td>
<td>March 2023</td>
</tr>
</tbody>
</table>
Warranty and support

Table of contents
- Limited warranty
- Disclaimer
- Customer support
- Customer service

Limited warranty

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

Disclaimer

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

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

Brand and product names are trademarks or registered trademarks of their respective owners.
©2023 by Kontron

Customer support

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

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

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. |

**Elevated operating ambient temperature**

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

**Reduced air flow**

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

**Mechanical loading**

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

**CE mark**

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

**Waste electrical and electronic equipment directive**

This product contains electrical or electronic materials. If not disposed of properly, these materials may have potential adverse effects on the environment and human health. The presence of this logo on the product means it should not be disposed of as unsorted waste and must be collected separately. Dispose of this product according to the appropriate local rules, regulations and laws.

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

**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 ground lug on the equipment.

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**

![Image of Earth ground lug location]

**Regulatory specifications**

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

**Safety compliance**
This product is marked cCSAus.

This product complies with the Low Voltage Directive 2014/35/EU and EN 62368-1.

This product has a CB report and certificate to IEC 62368-1.

Electromagnetic compatibility


This product complies with CISPR 32 Class A and CISPR 35.

This product complies with VCCI Class A. Note for Japan AC input rating is 90-130 VAC.

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI － A
Specifications

Table of contents
- ME1310 key hardware features
- ME1310 key software features
- ME1310 physical dimensions
- ME1310 packaging physical dimensions
- ME1310 shipping weights
- ME1310 environmental specifications

ME1310 key hardware features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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  
                           | Refer to the [Hardware compatibility list](#)  |
| 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

Version 1.0 (March 2023) // www.kontron.com
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform management</td>
<td>• BMC powered by OpenBMC&lt;br&gt;• UEFI based on AMI AptioV</td>
</tr>
<tr>
<td>Connectivity</td>
<td>• Dedicated or shared (NIC-SI) LAN interface&lt;br&gt;• USB LAN host interface (for Redfish)&lt;br&gt;• IPMI host interface (thru KCS)&lt;br&gt;• Remote management&lt;br&gt;• Redfish 1.9 + 2020.1 Schema&lt;br&gt;• IPMI 2.0 RMCP+&lt;br&gt;• Web UI&lt;br&gt;• Remote Access&lt;br&gt;• KVM/VM&lt;br&gt;• Serial interface over IPMI and SSH</td>
</tr>
<tr>
<td>Monitoring and power control</td>
<td>• Power control&lt;br&gt;• Power control&lt;br&gt;• Status&lt;br&gt;• Boot device override&lt;br&gt;• Cooling and heating&lt;br&gt;• Monitoring&lt;br&gt;• Thermal&lt;br&gt;• Power&lt;br&gt;• Humidity&lt;br&gt;• Board/device monitoring&lt;br&gt;• Telco alarm&lt;br&gt;• Logging and alerting (logs and events)</td>
</tr>
<tr>
<td>Configuration</td>
<td>• User management (internal, LDAP)&lt;br&gt;• Firmware management&lt;br&gt;• Version&lt;br&gt;• Update&lt;br&gt;• Signature validation&lt;br&gt;• Failsafe thru dual bank (available thru Redfish and Web UI)&lt;br&gt;• Network management (DHCP and static, VLAN)</td>
</tr>
<tr>
<td>Security</td>
<td>• Encryption (password encryption, TLS, IPMI Cipher 17)&lt;br&gt;• Authentication (LDAP / Active Directory)&lt;br&gt;• Firmware signature&lt;br&gt;• Secure boot&lt;br&gt;• CSM/legacy (available, but disabled by default)</td>
</tr>
<tr>
<td>Kontron Secure Edge</td>
<td>• Management Redfish/Web UI enabled&lt;br&gt;• Agent pre-provisioned</td>
</tr>
<tr>
<td>Operating system</td>
<td>Refer to the <a href="#">Validated operating systems</a></td>
</tr>
<tr>
<td>Thermal management</td>
<td>• Platform Environment Control Interface (PECI) for thermal management support&lt;br&gt;• Memory and CPU thermal management</td>
</tr>
</tbody>
</table>

**ME1310 physical dimensions**

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

**ME1310 packaging physical dimensions**

<table>
<thead>
<tr>
<th>Depth (mm [in])</th>
<th>Width (mm [in])</th>
<th>Height (mm [in])</th>
</tr>
</thead>
<tbody>
<tr>
<td>489 [19.25]</td>
<td>571.5 [22.5]</td>
<td>190.5 [7.5]</td>
</tr>
</tbody>
</table>
### ME1310 shipping weights

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

### ME1310 environmental specifications

<table>
<thead>
<tr>
<th>Environment</th>
<th>Specification</th>
</tr>
</thead>
</table>
| Temperature, operating | DC power supply: -40ºC to +65ºC (-40ºF to +149ºF)  
AC power supply: -5ºC to +50ºC (23ºF to +122ºF)  
The failure of one fan will not impact operation for at least 4 hours at 65 ºC.  
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 ºC to +85 ºC). |
| Temperature, non-operating | -40ºC to +70ºC (-40ºF to +158ºF) |
| 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/s² (0.0002 g²/Hz) (flat)  
- 50 Hz to 100 Hz at -12 dB/octave (slope down)  
- 30 minutes for each of the three axes |
| Vibration, non-operating | This product meets transportation and storage random vibration standards.  
Test profile based on GR-63 clause 5.4.3, and ETSI EN 300 019-2-2 class 2.3  
- 5 Hz to 20 Hz at 1 m²/s² (0.01 g²/Hz) (flat)  
- 20 Hz to 200 Hz at -3 dB/octave (slope down)  
- 30 minutes for each of the three axes |
| Shock, operating | This product meets operational shock standards.  
Test profile based on ETSI EN 300 019-2-3 class 3.2  
- 11 ms half sine, 3 g, three shocks in each direction |
| Drop/free fall | This product meets Bellcore GR-63 section 5.3.  
Packaged = 1,000 mm, six surfaces, three edges and four corners  
Unpackaged = 100 mm, two sides and two bottom corners |
| Electrostatic discharge | This product meets 8 kV contact, 15 kV air discharge using IEC 61000-4-2 test method. |
| RoHS and WEEE | This product is designed to meet China RoHS Phase 1 (self-declaration and labeling).  
This product complies with EU directive 2012/19/EU (WEEE).  
This product complies with RoHS directive 2011/65/EU as modified by EU 2015/863. |
Platform components

Table of contents
- Platform front panel
- Ethernet switch IO module option
- Pass-through IO module option
- Platform LEDs
- General platform LEDs
- Network port Srv 5 LEDs
- IO module network port LEDs
- Ethernet switch module
- Pass-through module
- Power supply LEDs
- DC power supply
- AC power supply
- Platform fans
- Platform label

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

<table>
<thead>
<tr>
<th>Status (amber/red)</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No active error notification (normal operation)</td>
</tr>
<tr>
<td>Amber On</td>
<td>Major alarm active</td>
</tr>
<tr>
<td>Red On</td>
<td>Critical alarm active (service/maintenance is required)</td>
</tr>
<tr>
<td>ID/preheat Indicator (blue)</td>
<td>Power (green)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Slow blink</td>
<td>Off</td>
</tr>
<tr>
<td>Normal blink</td>
<td>Any</td>
</tr>
<tr>
<td>Off</td>
<td>Rapid blink</td>
</tr>
<tr>
<td>Off</td>
<td>Normal blink</td>
</tr>
<tr>
<td>Off</td>
<td>Normal blink or On ¹</td>
</tr>
<tr>
<td>Off</td>
<td>On ¹</td>
</tr>
</tbody>
</table>

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

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

Network port Srv 5 LEDs

<table>
<thead>
<tr>
<th>Link (left – green/yellow)</th>
<th>Activity (right – green)</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Off</td>
<td>No link</td>
</tr>
<tr>
<td>Off</td>
<td>On (no activity)</td>
<td>10Base-T link established</td>
</tr>
<tr>
<td>Yellow On</td>
<td>On (no activity)</td>
<td>100Base-TX link established</td>
</tr>
<tr>
<td>Green On</td>
<td>On (no activity)</td>
<td>1000Base-T link established</td>
</tr>
</tbody>
</table>
IO module network port LEDs

Ethernet switch module

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

Pass-through module

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

Power supply LEDs

DC power supply

<table>
<thead>
<tr>
<th>Output status/operation (amber/green)</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Hot-swap controller Off or FPGA not loaded</td>
</tr>
<tr>
<td>Amber On</td>
<td>Hold-up not ready or voltage too low for start-up</td>
</tr>
<tr>
<td>Green On</td>
<td>Hold-up ready</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Input status/operation (amber/green)</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No 48V</td>
</tr>
<tr>
<td>Amber On</td>
<td>Hot-swap controller Off (low input voltage or fault)</td>
</tr>
<tr>
<td>Green On</td>
<td>Hot-swap controller On</td>
</tr>
</tbody>
</table>

AC power supply
### Input status/operation (green)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>Input voltage operating within normal specified range</td>
</tr>
<tr>
<td>Blinking</td>
<td>Input voltage operating in:</td>
</tr>
<tr>
<td></td>
<td>1) overvoltage warning, or</td>
</tr>
<tr>
<td></td>
<td>2) undervoltage warning</td>
</tr>
<tr>
<td>Off</td>
<td>Input voltage operating:</td>
</tr>
<tr>
<td></td>
<td>1) above overvoltage range, or</td>
</tr>
<tr>
<td></td>
<td>2) below undervoltage range, or</td>
</tr>
<tr>
<td></td>
<td>3) not present</td>
</tr>
</tbody>
</table>

### Output status/operation (amber/green)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green On</td>
<td>Power good mode: Main output and standby output enabled with no power supply warning or fault detected</td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Standby mode: Standby output enabled with no power supply warning or fault detected</td>
</tr>
<tr>
<td>Blinking Amber</td>
<td>Warning mode: Power supply warning detected as per PMBus STATUS_X reporting bytes</td>
</tr>
<tr>
<td>Amber On</td>
<td>Fault mode: Power supply fault detected as per PMBus STATUS_X reporting</td>
</tr>
</tbody>
</table>

### 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
ZZX1234HH (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 pass-through IO module option
- Network planes
  - Internal connections
    - Internal connections with the Ethernet switch IO module option
    - Internal connections with the pass-through IO module option

Block diagram

Block diagram with the Ethernet switch IO module option

Block diagram with the pass-through IO module option

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)
<table>
<thead>
<tr>
<th>Network planes</th>
<th>Description</th>
<th>Speed (GbE)</th>
<th>Component access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management plane</td>
<td>The management plane carries platform administrative traffic. This plane is used to support hardware management, configuration and health/thermal/power monitoring.</td>
<td>1</td>
<td>BMC</td>
</tr>
<tr>
<td>Control plane</td>
<td>The control plane carries customer application signaling traffic. This plane is used to control customer applications.</td>
<td>1</td>
<td>Server</td>
</tr>
<tr>
<td>Data plane</td>
<td>The data plane carries customer data application traffic. This plane is used to deliver service to end users.</td>
<td>1/10/25</td>
<td>Server, BMC, switch NOS</td>
</tr>
</tbody>
</table>

**Internal connections**

**Internal connections with the Ethernet switch IO module option**

![Ethernet switch IO module option diagram]

**Internal connections with the pass-through IO module option**

This option is planned for development. Please contact Kontron sales.
Description of system access methods

Table of contents
- Paths to the management interface (BMC)
- Paths to the operating system
- Paths to the UEFI/BIOS options
- Paths to the switch network operating system (NOS)

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)

<table>
<thead>
<tr>
<th>Path description</th>
<th>Main reasons for use</th>
</tr>
</thead>
</table>
| BMC Web UI       | - Remote server control and monitoring  
|                  | - OS video access  
|                  | - Firmware upgrades |
| Redfish          | - Remote server monitoring  
|                  | - Remote server control  
|                  | - Firmware upgrades |
| IPMI over LAN (IOL) | - Remote server control and monitoring |
| IPMI via KCS     | - 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

<table>
<thead>
<tr>
<th>Path description</th>
<th>Main reasons for use</th>
</tr>
</thead>
</table>
| KVM              | - 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 | - 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 | - OS network interface configuration  
|                  | - Unable to establish a network session to the OS  
|                  | - OS serial console access |
| Serial over LAN using IPMI from a remote computer | - OS network interface configuration  
|                  | - Unable to establish a network session to the OS  
|                  | - OS serial console access |
| SSH/RDP/Customer application protocols | - Operating the platform under normal operation  
|                  | - Remote access to the OS |
| Serial console (physical connection) | - Initial OS network interface configuration  
|                  | - No configuration performed on BMC  
|                  | - Troubleshooting |
Paths to the UEFI/BIOS options

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

<table>
<thead>
<tr>
<th>Paths to the UEFI/BIOS options</th>
<th>Main reasons for use</th>
</tr>
</thead>
</table>
| **Serial over LAN using the Web UI** | - Initial UEFI/BIOS configuration  
- UEFI/BIOS video access |
| **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. |  |
| **KVM** | - Initial UEFI/BIOS configuration  
- UEFI/BIOS video access |
| **Fail-safe** path to access the server if any elements (OS, UEFI/BIOS, etc.) get misconfigured. Accessible from the BMC management plane. |  |
| **Serial over LAN using SSH from a remote computer** | - Initial UEFI/BIOS configuration  
- UEFI/BIOS serial console access  
- OS network interfaces not configured, but BMC network access is available |
| **Accessible from the BMC management plane.** |  |
| **Serial over LAN using IPMI from a remote computer** | - Initial UEFI/BIOS configuration  
- UEFI/BIOS serial console access  
- OS network interfaces not configured, but BMC network access is available |
| **Accessible from the BMC management plane.** |  |
| **Redfish** | - Basic UEFI/BIOS configuration |
| **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.** |  |
| **Serial console (physical connection)** | - Initial UEFI/BIOS configuration  
- No configuration performed on BMC  
- Troubleshooting |
| **Fail-safe path to access all server components when elements (OS, BMC, UEFI/BIOS, etc.) get misconfigured. Accessible from the physical port.** |  |

*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.

<table>
<thead>
<tr>
<th>Paths to the switch network operating system (NOS)</th>
<th>Main reasons for use</th>
</tr>
</thead>
</table>
| **Switch NOS Web UI** | - Switch NOS control and monitoring  
- Firmware upgrades |
| **This is the recommended path for first time out-of-the-box system configuration.** |  |
| **Accessible from the data plane.** |  |
| **Serial over LAN using the BMC Web UI** | - NOS network interface configuration  
- Initial switch NOS configuration |
| **Accessible from the BMC management plane.** |  |
| **Serial over LAN using SSH from a remote computer** | - NOS network interface configuration  
- Initial switch NOS configuration |
| **Accessible from the BMC management plane.** |  |
| **SSH from a remote computer** | - Switch NOS control and monitoring  
- Firmware upgrades |
| **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.** |  |
| **SSH from the integrated server** | - Local access to the switch NOS for control and monitoring |
| **Accessible locally from the server operating system.** |  |

*Note that communication with the BMC management plane via the integrated switch can be lost because of configurations applied in the NOS.
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 -40°C to +65°C (-40°F to +149°F) when using a DC power supply or -5°C to +50°C (23°F to +122°F) when using an AC power supply and to withstand non-condensing humidity levels up to 95%. This equipment should not be exposed directly to the elements (sun, rain, wind, dust). For installations in outdoor or other harsh, uncontrolled environments, 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. Once powered up and in operation, the system will dissipate enough power to stay warm. The warm-up delay of the deep cold start is a rare event that could occur only at the initial power up or after a power outage in a cold environment.

Special considerations must be taken if you are exposing the 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
- AC power supply input voltage and current requirements
- Power consumption examples
  - System power consumption
  - Component power consumption examples

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 B) and intra-cell site DC power limited outdoor exposure (type 8b).

AC power supply input voltage and current requirements

<table>
<thead>
<tr>
<th>AC input voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal</td>
</tr>
<tr>
<td>Minimum</td>
</tr>
<tr>
<td>Maximum</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AC input current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Power input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
</tr>
</tbody>
</table>

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 SATA module
- Two 25GBASE-LR SFP28 modules
- Two 10GBASE-SR SFP+ modules
- Two PCIe add-in cards: 75 W power test jigs
- DC PSU
- Standard 8 fans

<table>
<thead>
<tr>
<th>Status</th>
<th>Typical consumption (W)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>78</td>
<td>Idle power consumption was measured in CentOS 7 once it had finished booting</td>
</tr>
<tr>
<td>Maximum application</td>
<td>342</td>
<td>Maximum power was measured in CentOS 7 running “imprime -t” as a stress application</td>
</tr>
<tr>
<td>Maximum application and fan</td>
<td>500</td>
<td>Maximum power was measured in CentOS 7 running “imprime -t” as a stress application with fans at maximum speed</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Components</th>
<th>Typical consumption (W)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel® Xeon® D-2796NT</td>
<td>120</td>
<td>TDP</td>
</tr>
<tr>
<td>Intel® Xeon® D-2776NT</td>
<td>117</td>
<td>TDP</td>
</tr>
<tr>
<td>Intel® Xeon® D-2766NT</td>
<td>97</td>
<td>TDP</td>
</tr>
<tr>
<td>Ethernet switch IO module with standard OCXO</td>
<td>23</td>
<td>Ethernet switch has 4 SFP interfaces with link up</td>
</tr>
<tr>
<td>Fans</td>
<td>23</td>
<td>At maximum speed</td>
</tr>
<tr>
<td>64 GB LRDIMM</td>
<td>6</td>
<td>Under active use</td>
</tr>
<tr>
<td>16 GB RDIMM</td>
<td>3.5</td>
<td>Under active use</td>
</tr>
<tr>
<td>NVMe 128GB, 512GB, 1TB or 2TB M.2 SSD</td>
<td>7</td>
<td>Under active use. Idle power is 1 W.</td>
</tr>
<tr>
<td>25GBASE-LR SFP28</td>
<td>1</td>
<td>Connection is link up with partner device</td>
</tr>
<tr>
<td>10GBASE-SR SFP+</td>
<td>1</td>
<td>Connection is link up with partner device</td>
</tr>
</tbody>
</table>

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

Table of contents
- MAC addresses
- Ethernet switch IO module option
- Pass-through IO module option
- Discovering the platform MAC addresses
  - Discovering a MAC address using the QR code
  - Discovering a MAC address using the UEFI/BIOS

Relevant section: Product architecture

MAC addresses

Ethernet switch IO module option

<table>
<thead>
<tr>
<th>MAC address</th>
<th>Interface description</th>
<th>Device</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_BASE</td>
<td>Front panel Srv 5</td>
<td>BMC</td>
<td>Shared connector with server.</td>
</tr>
<tr>
<td>MAC_BASE + 1</td>
<td>Server internal port 4</td>
<td>BMC</td>
<td>Internal to switch interface 1/16. Shared connection with server.</td>
</tr>
<tr>
<td>MAC_BASE + 2</td>
<td>Server Redfish host interface</td>
<td>Server</td>
<td>Internal to BMC via integrated USB-LAN.</td>
</tr>
<tr>
<td>MAC_BASE + 3</td>
<td>Server internal port 1</td>
<td>Server</td>
<td>Internal to switch interface 1/13.</td>
</tr>
<tr>
<td>MAC_BASE + 4</td>
<td>Server internal port 2</td>
<td>Server</td>
<td>Internal to switch interface 1/14.</td>
</tr>
<tr>
<td>MAC_BASE + 5</td>
<td>Server internal port 3</td>
<td>Server</td>
<td>Internal to switch interface 1/15.</td>
</tr>
<tr>
<td>MAC_BASE + 6</td>
<td>Server internal port 4</td>
<td>Server</td>
<td>Internal to switch interface 1/16. Shared connection with BMC.</td>
</tr>
<tr>
<td>MAC_BASE + 7</td>
<td>Front panel Srv 5</td>
<td>Server</td>
<td>Server control plane. Shared connection with BMC.</td>
</tr>
<tr>
<td>SW_MAC_BASE</td>
<td>Any switch interface</td>
<td>Switch</td>
<td>MAC used by the switch network operating system for configuration/monitoring access.</td>
</tr>
<tr>
<td>SW_MAC_BASE + 1</td>
<td>Reserved</td>
<td>Switch</td>
<td>Reserved MAC for switch network operating system.</td>
</tr>
</tbody>
</table>

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 screenshot).

| 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. |

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.

Version 1.0 (March 2023)
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 **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

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

<table>
<thead>
<tr>
<th>Bus: Device: Function</th>
<th>Vendor ID</th>
<th>Device ID</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00.0</td>
<td>8086</td>
<td>09a2</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:00.1</td>
<td>8086</td>
<td>09a4</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:00.2</td>
<td>8086</td>
<td>09a3</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:00.3</td>
<td>8086</td>
<td>09a5</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:00.4</td>
<td>8086</td>
<td>0998</td>
<td>Host bridge</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:01.0</td>
<td>8086</td>
<td>0b00</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:01.1</td>
<td>8086</td>
<td>0b00</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:01.2</td>
<td>8086</td>
<td>0b00</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:01.3</td>
<td>8086</td>
<td>0b00</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:01.4</td>
<td>8086</td>
<td>0b00</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:01.5</td>
<td>8086</td>
<td>0b00</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:01.6</td>
<td>8086</td>
<td>0b00</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:01.7</td>
<td>8086</td>
<td>0b00</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:02.0</td>
<td>8086</td>
<td>09a6</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:02.1</td>
<td>8086</td>
<td>09a7</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:02.4</td>
<td>8086</td>
<td>3456</td>
<td>Non-Essential Instrumentation</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:09.0</td>
<td>8086</td>
<td>18a4</td>
<td>PCI bridge</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:0b.0</td>
<td>8086</td>
<td>18a6</td>
<td>PCI bridge</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:0f.0</td>
<td>8086</td>
<td>18ac</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:16.0</td>
<td>8086</td>
<td>18af</td>
<td>PCI bridge</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:17.0</td>
<td>8086</td>
<td>18a2</td>
<td>PCI bridge</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:18.0</td>
<td>8086</td>
<td>18d3</td>
<td>Communication controller</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:18.1</td>
<td>8086</td>
<td>18d4</td>
<td>Communication controller</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:18.4</td>
<td>8086</td>
<td>18d6</td>
<td>Communication controller</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1a.0</td>
<td>8086</td>
<td>18d8</td>
<td>Serial controller</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1a.1</td>
<td>8086</td>
<td>18d8</td>
<td>Serial controller</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1a.2</td>
<td>8086</td>
<td>18d8</td>
<td>Serial controller</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1a.3</td>
<td>8086</td>
<td>18d9</td>
<td>Unassigned class</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1d.0</td>
<td>8086</td>
<td>099b</td>
<td>Host bridge</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1e.0</td>
<td>8086</td>
<td>18d0</td>
<td>USB controller</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1f.0</td>
<td>8086</td>
<td>18dc</td>
<td>ISA bridge</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1f.4</td>
<td>8086</td>
<td>18df</td>
<td>SMBus</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1f.5</td>
<td>8086</td>
<td>18e0</td>
<td>Serial bus controller</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>00:1f.7</td>
<td>8086</td>
<td>18e1</td>
<td>Non-Essential Instrumentation</td>
<td>Intel Corporation Device</td>
</tr>
<tr>
<td>01:00.0</td>
<td>1d79</td>
<td>2263</td>
<td>Non-Volatile memory controller</td>
<td>Transcend Information, Inc. Device</td>
</tr>
<tr>
<td>Device ID</td>
<td>Function</td>
<td>Manufacturer</td>
<td>Model</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>--------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>02:00.0</td>
<td>1a03 1150</td>
<td>PCI bridge</td>
<td>ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge</td>
<td></td>
</tr>
<tr>
<td>03:00.0</td>
<td>1a04 6001</td>
<td>Non-Volatile memory controller</td>
<td>Micron Technology Inc Device</td>
<td></td>
</tr>
<tr>
<td>04:00.0</td>
<td>8086 1533</td>
<td>Ethernet controller</td>
<td>Intel Corporation I210 Gigabit Network Connection</td>
<td></td>
</tr>
<tr>
<td>05:00.0</td>
<td>1a03 2000</td>
<td>VGA compatible controller</td>
<td>ASPEED Technology, Inc. ASPEED Graphics Family</td>
<td></td>
</tr>
<tr>
<td>15:00.0</td>
<td>8086 09a2</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>15:00.1</td>
<td>8086 09a4</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>15:00.2</td>
<td>8086 09a3</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>15:00.3</td>
<td>8086 09a5</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>15:00.4</td>
<td>8086 0998</td>
<td>Host bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>15:02.0</td>
<td>8086 347a</td>
<td>PCI bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>16:00.0</td>
<td>8086 0d5c</td>
<td>Processing accelerators</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>80:00.0</td>
<td>8086 09a2</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>80:00.1</td>
<td>8086 09a4</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>80:00.2</td>
<td>8086 09a3</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>80:00.3</td>
<td>8086 09a5</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>80:00.4</td>
<td>8086 0998</td>
<td>Host bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>80:05.0</td>
<td>8086 18da</td>
<td>PCI bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>81:00.0</td>
<td>8086 18a0</td>
<td>Co-processor</td>
<td>Intel Corporation C4xxx Series QAT</td>
<td></td>
</tr>
<tr>
<td>88:00.0</td>
<td>8086 09a2</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>88:00.1</td>
<td>8086 09a4</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>88:00.2</td>
<td>8086 09a3</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>88:00.3</td>
<td>8086 09a5</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>88:00.4</td>
<td>8086 0998</td>
<td>Host bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>88:04.0</td>
<td>8086 18d1</td>
<td>PCI bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>89:00.0</td>
<td>8086 188a</td>
<td>Ethernet controller</td>
<td>Intel Corporation Ethernet Connection EB23-C for backplane</td>
<td></td>
</tr>
<tr>
<td>89:00.1</td>
<td>8086 188a</td>
<td>Ethernet controller</td>
<td>Intel Corporation Ethernet Connection EB23-C for backplane</td>
<td></td>
</tr>
<tr>
<td>89:00.2</td>
<td>8086 188a</td>
<td>Ethernet controller</td>
<td>Intel Corporation Ethernet Connection EB23-C for backplane</td>
<td></td>
</tr>
<tr>
<td>89:00.3</td>
<td>8086 188a</td>
<td>Ethernet controller</td>
<td>Intel Corporation Ethernet Connection EB23-C for backplane</td>
<td></td>
</tr>
<tr>
<td>90:00.0</td>
<td>8086 09a2</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>90:00.1</td>
<td>8086 09a4</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>90:00.2</td>
<td>8086 09a3</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>90:00.3</td>
<td>8086 09a5</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>90:00.4</td>
<td>8086 0998</td>
<td>Host bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>90:02.0</td>
<td>8086 347a</td>
<td>PCI bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:00.0</td>
<td>8086 3450</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:00.1</td>
<td>8086 3451</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:00.2</td>
<td>8086 3452</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:00.3</td>
<td>8086 0998</td>
<td>Host bridge</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:00.5</td>
<td>8086 3455</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:0b.0</td>
<td>8086 344b</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:0b.1</td>
<td>8086 344b</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:0b.2</td>
<td>8086 344b</td>
<td>System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:0c.0</td>
<td>8086 344a</td>
<td>Performance counters</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:0d.0</td>
<td>8086 344a</td>
<td>Performance counters</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>fe:1a.0</td>
<td>8086 2880</td>
<td>Performance</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>Code</td>
<td>Description</td>
<td>Device Type</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>-------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>fe:1b.0</td>
<td>8086</td>
<td>2880 Performance counters</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:00.0</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:00.1</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:00.2</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:00.3</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:00.4</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:00.5</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:00.6</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:00.7</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:01.0</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:01.1</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:01.2</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:01.3</td>
<td>8086</td>
<td>344c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0a.0</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0a.1</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0a.2</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0a.3</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0a.4</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0a.5</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0a.6</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0a.7</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0b.0</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0b.1</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0b.2</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:0b.3</td>
<td>8086</td>
<td>344d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1d.0</td>
<td>8086</td>
<td>344f System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1d.1</td>
<td>8086</td>
<td>3457 System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1e.0</td>
<td>8086</td>
<td>3458 System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1e.1</td>
<td>8086</td>
<td>3459 System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1e.2</td>
<td>8086</td>
<td>345a System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1e.3</td>
<td>8086</td>
<td>345b System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1e.4</td>
<td>8086</td>
<td>345c System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1e.5</td>
<td>8086</td>
<td>345d System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1e.6</td>
<td>8086</td>
<td>345e System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
<tr>
<td>ff:1e.7</td>
<td>8086</td>
<td>345f System peripheral</td>
<td>Intel Corporation Device</td>
<td></td>
</tr>
</tbody>
</table>
Connector pinouts and electrical characteristics

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

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

Relevant sections:
- Platform components
- Cabling

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

**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
- RJ45 alarm port
- RJ45 serial port
- SFP+ and SFP28 ports
- RJ45 Ethernet management port
- USB interfaces
- DC power supply input connector
- AC power supply input connector
SMA GNSS RF input

Mating connector: SMA Male

Description:
- 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 dBi 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 \( I_{OL} = 12 \, mA \)
- Suitable for use with 50 ohms to ground terminated loads:
  - \( V_{OH} > 1.2 \, V \)
  - \( V_{OL} < 0.3 \, V \)
- PPS rising edge (at SMA) aligned within ± 5 ns from internal time of day (ToD) counter

RJ45 alarm port

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

Open circuit voltage:
- ALARM_CM: 5 V to 7 V, current limited to < 60 mA
- ALARM_IN[7:1]: -7 V to -5 V, 10 kilohms impedance

External connector pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal description</th>
<th>Pin</th>
<th>Signal description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ALARM_IN[1]</td>
<td>5</td>
<td>ALARM_IN[5]</td>
</tr>
<tr>
<td>3</td>
<td>ALARM_IN[3]</td>
<td>7</td>
<td>ALARM_IN[7]</td>
</tr>
<tr>
<td>4</td>
<td>ALARM_IN[4]</td>
<td>8</td>
<td>ALARM_CM</td>
</tr>
</tbody>
</table>

Relevant sections:
- Discrete sensor monitoring procedure
- Interpreting sensor data

RJ45 serial port

![RJ45 serial port diagram]

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

External connector pinout:

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal description</th>
<th>Pin</th>
<th>Signal description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RTS</td>
<td>5</td>
<td>GND</td>
</tr>
<tr>
<td>2</td>
<td>DTR</td>
<td>6</td>
<td>RX#</td>
</tr>
<tr>
<td>3</td>
<td>TX#</td>
<td>7</td>
<td>DSR</td>
</tr>
<tr>
<td>4</td>
<td>GND</td>
<td>8</td>
<td>CTS</td>
</tr>
</tbody>
</table>

SFP+ and SFP28

Ethernet switch IO module option

![Ethernet switch IO module diagram]

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**

![RJ45 Ethernet management port](image)

**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**

![USB interfaces](image)

**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](https://www.usb.org).

**DC power supply input connector**

![DC power supply input connector](image)

**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)
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 Bb).

## 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 A pk)
  - 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
  - Optional adapter
  - Component installation and assembly
    - PCIe add-in card
  - Power cables and tooling
    - For a DC PSU
    - For an AC PSU
  - Rack installation material
  - Network cables and modules
    - Ethernet switch I/O module option
    - Pass-through I/O module option
  - Software required

Material and information required

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

Optional adapter

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

Component installation and assembly

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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>One T10 Torx screwdriver</td>
</tr>
<tr>
<td>Item_2</td>
<td>(Optional) One thermal probe for temperature monitoring (if physical temperature monitoring is chosen)</td>
</tr>
<tr>
<td>Item_3</td>
<td>(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)</td>
</tr>
</tbody>
</table>

Power cables and tooling

For a DC PSU
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)

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

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 lugs
  OR
- Maximum insulation diameter: 5.8 mm [0.23 in] for Panduit crimp lugs

One hand crimp tool:
- Molex Premium Grade Hand Crimp Tool (640010100)
  OR
- Panduit Hand Crimp Tool (638130400)

One 8 AWG ground cable based on the length required

One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)

One hand crimp tool, Panduit CT-1700

7 mm wrench or equivalent tool

For an AC PSU

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

Racking fasteners (rack specific)

Network cables and modules

Ethernet switch IO module option

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

One RJ45 Ethernet management/control plane cable

One RJ45 serial connection cable

Pass-through IO module option

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

Software required

An HTTP client such as cURL or Postman is recommended for using the platform Redfish interface. Throughout the documentation, cURL will be used.

A terminal emulator such as PuTTY is installed on a remote computer.

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

A 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.

<table>
<thead>
<tr>
<th>Description</th>
<th>Kontron P/N</th>
<th>Illustration</th>
</tr>
</thead>
<tbody>
<tr>
<td>RJ45 to DB9 serial adapter</td>
<td>1015-9404</td>
<td><img src="image1.png" alt="RJ45 to DB9 serial adapter" /></td>
</tr>
<tr>
<td>C13 to CEE 7/7 European AC power cord, 10A/250 VAC, 1.8 m long</td>
<td>1061-0410</td>
<td><img src="image2.png" alt="C13 to CEE 7/7 European AC power cord" /></td>
</tr>
<tr>
<td>C13 to NEMA 5-15P AC power cord, 10A/125 VAC, 2 m long</td>
<td>1-340000-0</td>
<td><img src="image3.png" alt="C13 to NEMA 5-15P AC power cord" /></td>
</tr>
<tr>
<td>Ground lug right angle, 8 AWG</td>
<td>1064-4226</td>
<td><img src="image4.png" alt="Ground lug right angle" /></td>
</tr>
<tr>
<td>Thermal probe for PCIe add-in card</td>
<td>1065-9296</td>
<td><img src="image5.png" alt="Thermal probe for PCIe add-in card" /></td>
</tr>
</tbody>
</table>
# Hardware Compatibility List

## Table of Contents
- M.2 industrial SSDs (-40°C to 85°C)
- Memory RDIMM ECC industrial modules (-40°C to 85°C)
- SFP, SFP+ and SFP28 industrial modules (-40°C to 85°C)

## M.2 Industrial SSDs (-40°C to 85°C)

<table>
<thead>
<tr>
<th>Type</th>
<th>Size</th>
<th>Dimension</th>
<th>Vendor</th>
<th>Vendor P/N</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVMe</td>
<td>128GB</td>
<td>2280</td>
<td>Transcend</td>
<td>TS128GMTE652TI</td>
<td>Active</td>
<td>1068-6586</td>
</tr>
<tr>
<td>NVMe</td>
<td>512GB</td>
<td>2280</td>
<td>Transcend</td>
<td>TS512GMTE652TI-KCI</td>
<td>Active</td>
<td>1068-1170</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Western Digital</td>
<td>SDBPnPZ-51G-XI</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>NVMe</td>
<td>1TB</td>
<td>2280</td>
<td>Transcend</td>
<td>TS1TMTE662TI-KCI</td>
<td>Active</td>
<td>1068-1161</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Western Digital</td>
<td>SDBPnPZ-1T00-XI</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>NVMe</td>
<td>2TB</td>
<td>2280</td>
<td>Transcend</td>
<td>TS2TMTE662TI-KCI</td>
<td>Active</td>
<td>1068-1158</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Western Digital</td>
<td>SDBPnPZ-2T00-XI</td>
<td>Active</td>
<td></td>
</tr>
</tbody>
</table>

## Memory RDIMM ECC Industrial Modules (-40°C to 85°C)

<table>
<thead>
<tr>
<th>Size</th>
<th>Type</th>
<th>Vendor</th>
<th>Vendor P/N</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>16GB</td>
<td>DDR4-3200*</td>
<td>Micron Technology</td>
<td>MTA18ASF2G72PD8Z-3G2E1</td>
<td>Active</td>
<td>1067-0181</td>
</tr>
<tr>
<td>32GB</td>
<td>DDR4-3200*</td>
<td>Micron Technology</td>
<td>MTA36ASF4G72PBZ-3G2E1</td>
<td>Active</td>
<td>1068-6284</td>
</tr>
<tr>
<td>64GB</td>
<td>DDR4-3200*</td>
<td>Smart Modular Technology</td>
<td>STI8197RD440425-SA</td>
<td>Active</td>
<td>1068-6291</td>
</tr>
</tbody>
</table>

*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

<table>
<thead>
<tr>
<th>Type</th>
<th>Vendor</th>
<th>Vendor P/N</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000BASE-SX</td>
<td>II-VI (Finisar)</td>
<td>FTLF8519F3BTL</td>
<td>500m, 850nm, -40°C to 85°C, SFP optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td>10GBASE-SR</td>
<td>II-VI (Finisar)</td>
<td>FTLX8573D3BTL</td>
<td>400m, 850nm, -40°C to 85°C, SFP+ optical transceiver</td>
<td>EOL</td>
</tr>
<tr>
<td></td>
<td>II-VI (Finisar)</td>
<td>FTLX8574D3BTL</td>
<td>400m, 850nm, -40°C to 85°C, SFP+ optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>FormericaOE</td>
<td>TAS-A2NH1-P11</td>
<td>300m, 850nm, -40°C to 85°C, SFP+ optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td>25GBASE-SR</td>
<td>FS</td>
<td>SFP28-25GSR-85-I</td>
<td>100m, 850nm, -40°C to 85°C, SFP28 optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>II-VI (Finisar)</td>
<td>FTLF8536W4BTV</td>
<td>100m, 850nm, -40°C to 85°C, SFP28 optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td>1000BASE-LX</td>
<td>FormericaOE</td>
<td>TSO-S2CA1-F11</td>
<td>10Km, 1310nm, -40°C to 85°C, SFP optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>II-VI (Finisar)</td>
<td>FTLF131BP3BTL</td>
<td>10Km, 1310nm, -40°C to 85°C, SFP optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>Avago</td>
<td>AFCT-5715ALZ</td>
<td>10Km, 1310nm, -40°C to 85°C, SFP optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td>10GBASE-LR</td>
<td>FS</td>
<td>SFP-10GLR-31-I</td>
<td>10Km, 1310nm, -40°C to 85°C, SFP+ optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>II-VI (Finisar)</td>
<td>FTLX1475D3BTL</td>
<td>10Km, 1310nm, -40°C to 85°C, SFP+ optical transceiver</td>
<td>Active</td>
</tr>
<tr>
<td>25GBASE-LR</td>
<td>FS</td>
<td>SFP28-25GLR-31-I</td>
<td>10Km, 1310nm, -40°C to 85°C, SFP28 optical transceiver</td>
<td>Active</td>
</tr>
</tbody>
</table>
Validated operating systems

Table of contents
• Status description
• OS certification status

Status description

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

OS certification status

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

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 7.8</td>
<td>PLANNED</td>
</tr>
<tr>
<td>RHEL 7.8</td>
<td>PLANNED</td>
</tr>
<tr>
<td>RHEL 8.2</td>
<td>PLANNED</td>
</tr>
<tr>
<td>SUSE EL 15 SP2</td>
<td>PLANNED</td>
</tr>
<tr>
<td>Ubuntu 18.04</td>
<td>PLANNED</td>
</tr>
<tr>
<td>Ubuntu 20.04</td>
<td>PLANNED</td>
</tr>
<tr>
<td>VMWare ESXi 6.7</td>
<td>PLANNED</td>
</tr>
</tbody>
</table>
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
Getting started - Application installation and performance benchmarking

Table of contents
- Safety and regulatory information
- Introduction
- Unboxing the platform
- What’s in the box
- Planning
  - Material and information required
  - Software required
- Installing one or two PCIe add-in cards and thermal probes in an ME1310
  - Opening the chassis
  - Installing one or two thermal probes for the PCIe add-in cards
  - Connecting one or two PCIe add-in cards
  - Closing the chassis
- Racking the platform
- Connecting the network cables
- Procedure
- Discovering the BMC IP address
  - Accessing the UEFI/BIOS using a serial console (physical connection)
  - Accessing the BMC network configuration menu
- Discovering the switch NOS IP address
  - Discovering the switch NOS IP address through the switch NOS serial console CLI
- Prepare for operating system installation
- Installing an operating system using the KVM
  - Prerequisites
  - Browser considerations
  - Connecting to the Web UI of the BMC
  - Launching the KVM
  - Mounting the operating system image via virtual media
  - Accessing the UEFI/BIOS setup menu
  - Selecting the boot order from boot override
  - Completing operating system installation
- Verifying operating system installation
- Benchmarking an application
- Monitoring platform sensors
  - Monitoring platform sensors using the Web UI

Safety and regulatory information

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

Introduction

This getting started section describes the network integration, platform access and operating system installation steps required to start operating an ME1310 platform equipped with one or two PCIe add-in cards provided by the customer and one 128GB M.2 SATA drive, and used to leverage two segregated network links (one for the management/control plane and one for the data plane).

This use case is based on a simplified architecture with one management plane, one control plane and one data plane.

Assumptions

The scenario described in this getting started section is based on the following assumptions:
- The network connections of the system are as follows:
  - One management plane (red line) and one control plane (green line) via the RJ45 management port 5 (Srv 5)
  - One data plane (purple line) via SFP 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)
- 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
- 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 lugs
- Maximum insulation diameter: 5.8 mm [0.23 in] for Panduit crimp lugs

### Item 4
One hand crimp tool:
- Molex Premium Grade Hand Crimp Tool (640010100)
- 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.

<table>
<thead>
<tr>
<th>Location</th>
<th>Reference designator</th>
<th>Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back</td>
<td>J20</td>
<td>PCIe slot 1</td>
</tr>
<tr>
<td>Middle</td>
<td>J21</td>
<td>PCIe slot 2</td>
</tr>
<tr>
<td>Front</td>
<td>J23</td>
<td>Chassis</td>
</tr>
</tbody>
</table>

Version 1.0 (March 2023) www.kontron.com // 47
Installing the thermal probes

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>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.</td>
</tr>
<tr>
<td>Step_2</td>
<td>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. <strong>NOTE:</strong> Configuration will be performed once the platform is operational (thresholds, specific software configurations, etc.).</td>
</tr>
<tr>
<td>Step_3</td>
<td>Repeat steps 1 and 2 if two thermal probes must be installed.</td>
</tr>
</tbody>
</table>

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 and 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, fasten the blank L-bracket(s) to the PCIe holder (6 lbf·in torque). Mount the PCIe rear holder onto the assembly and tighten the M3 screws with a T10 Torx screwdriver (6 lbf·in torque).

**NOTE:** If the PCIe add-in cards do not comply with PCIe Electromechanical Specifications for rear keepouts, discard the PCIe rear holder.

### Step 4
Carefully insert the PCIe assembly into the unit and fasten the two thumbscrews (6 lbf·in torque). Connect the intrusion detection switch wire near the front of the chassis.

---

**Closing the chassis**
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.
Connecting the network cables

Connect the network cables according to the image below.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect one RJ45 cable to port 5 for the management and the control planes (Srv 5).</td>
</tr>
<tr>
<td>2</td>
<td>Connect one SFP or SFP+ cable to switch port 1 for the data plane (Sw 1).</td>
</tr>
</tbody>
</table>

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.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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).</td>
</tr>
<tr>
<td>2</td>
<td>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).</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Bend the crimp lugs to a 45° angle as shown in the image.</td>
</tr>
<tr>
<td>5</td>
<td>Remove the screw from the terminal block RTN “B” location.</td>
</tr>
<tr>
<td>6</td>
<td>Insert the crimped red wire in the RTN “B” location as shown in the image.</td>
</tr>
<tr>
<td>7</td>
<td>Screw the crimp lug in place.</td>
</tr>
<tr>
<td>8</td>
<td>Remove the screw from the terminal block -48V DC “B” location.</td>
</tr>
<tr>
<td>9</td>
<td>Insert the crimped black wire in the -48V DC “B” location as shown in the image.</td>
</tr>
<tr>
<td>10</td>
<td>Screw the crimp lug in place.</td>
</tr>
<tr>
<td>11</td>
<td>(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.</td>
</tr>
<tr>
<td>12</td>
<td>The power supply is reverse polarity protected. The unit will power on as soon as external power is applied (green power LED).</td>
</tr>
</tbody>
</table>

Discovering the BMC IP address

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

Relevant section:
Discovering platform IP addresses

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

Prerequisites

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 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 to 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 start the HTTPS self-signed certificate acceptance process. Information on the error message will be displayed.

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

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

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** 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.
**Benchmarking an application**

Install your application and proceed with benchmarking.

**Monitoring platform sensors**

Platform sensors can be monitored using various methods, including the 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.

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

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

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

What's in the box

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Carefully remove the platform from its packaging.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Remove the plastic film from the platform. <strong>Failure to do so may affect platform airflow efficiency, thus resulting in poor cooling capabilities.</strong></td>
</tr>
</tbody>
</table>
Components installation and assembly

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

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.

<table>
<thead>
<tr>
<th>Location</th>
<th>Reference designator</th>
<th>Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back</td>
<td>J20</td>
<td>PCIe slot 1</td>
</tr>
<tr>
<td>Middle</td>
<td>J21</td>
<td>PCIe slot 2</td>
</tr>
<tr>
<td>Front</td>
<td>J23</td>
<td>Chassis</td>
</tr>
</tbody>
</table>
(Optional) Building a thermal probe

<table>
<thead>
<tr>
<th>Component</th>
<th>P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTC thermistor</td>
<td>GA10K3A11A</td>
<td>NTC thermistor 10 Kohm, 3976K Bead</td>
</tr>
<tr>
<td>Connector</td>
<td>XHP-2</td>
<td>Connector housing 2.5 mm, 2 position</td>
</tr>
<tr>
<td>Pins</td>
<td>SXH-001-P0.6</td>
<td>Socket contact, 22-28 awg, crimp stamped</td>
</tr>
</tbody>
</table>

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 and 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, fasten the blank L-bracket(s) to the PCIe holder (6 lbf·in torque).
Mount the PCIe rear holder onto the assembly and tighten the M3 screws with a T10 Torx screwdriver (6 lbf·in torque).
NOTE: If the PCIe add-in cards do not comply with PCIe Electromechanical Specifications for rear keepouts, discard the PCIe rear holder.

Step_4
Carefully insert the PCIe assembly into the unit and fasten the two thumbscrews (6 lbf·in torque).
Connect the intrusion detection switch wire near the front of the chassis.

(Optional) Software installation instructions
Refer to 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 lbf·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

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

### Replacing fans

There are eight fans in this platform.

### Locating the fans

### Replacing a fan
### Replacing the RTC battery

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disconnect the fan connector.</td>
</tr>
<tr>
<td>2</td>
<td>Lift the fan up to take it out of the platform.</td>
</tr>
<tr>
<td>3</td>
<td>Insert a new fan and connect the fan connector.</td>
</tr>
</tbody>
</table>

**CAUTION**

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

### Locating the RTC battery

![Image of battery location](image)

### Replacing the battery

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>Safely dispose of the battery.</td>
</tr>
<tr>
<td>3</td>
<td>With one hand, gently push the latch and insert a new battery with the other hand. Respect the appropriate orientation and polarity.</td>
</tr>
</tbody>
</table>

### Closing the enclosure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Place the cover onto the chassis.</td>
</tr>
</tbody>
</table>
| 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 platform in a 19-in rack

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Choose a location for the platform in the rack.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Insert the platform in the rack.</td>
</tr>
<tr>
<td>Step_3</td>
<td>Fasten the platform to the rack using the appropriate fasteners.</td>
</tr>
<tr>
<td>Step_4</td>
<td>If a ground lug is installed, remove the 2 nuts and washers from the ground lug studs. Take out the ground lug.</td>
</tr>
<tr>
<td>Step_5</td>
<td>Strip 19 mm (0.75 in) of the 8 AWG ground cable.</td>
</tr>
<tr>
<td>Step_6</td>
<td>Insert the 8 AWG ground cable in the ground lug. Crimp the lug on the cable using an appropriate hand crimp tool (e.g. Panduit CT-1700 crimp tool set at: Color Code = Red; Die Index No. = P21).</td>
</tr>
<tr>
<td>Step_7</td>
<td>Install the ground lug on the studs, fastening with the 2 nuts and washers.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The thread of the two chassis ground lugs is M4x0.7.</td>
</tr>
</tbody>
</table>
Cabling

Table of contents
- DC power supply inlet
- Preparing the DC power supply cables
  - Material required
  - Procedure
- AC power supply inlet
  - Power cord usage guidelines
  - AC power supply connection
- GNSS input
  - Connecting to an RF splitter
  - Connecting to an external antenna

DC power supply inlet

<table>
<thead>
<tr>
<th>Description</th>
<th>Maximum input current</th>
<th>PSU receptacle model</th>
</tr>
</thead>
<tbody>
<tr>
<td>600 W DC power supply module input connector</td>
<td>17 A</td>
<td>Amphenol (Anytek) YK605042300G</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Manufacturer P/N</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crimp lugs:</td>
<td>2 (or 4 for redundancy)</td>
<td>1931-0023 or equivalent</td>
<td>Molex product catalog</td>
</tr>
<tr>
<td>- Molex insulated spade crimp lugs for 14-16 wire gauge</td>
<td></td>
<td></td>
<td>Part details</td>
</tr>
<tr>
<td>- Panduit insulated ring crimp lugs for 10-12 wire gauge</td>
<td></td>
<td>EV10-6RB-Q or equivalent</td>
<td>Panduit product catalog</td>
</tr>
<tr>
<td>- Black stranded wire to build the power cable based on the length required:</td>
<td>Length required</td>
<td></td>
<td>Part drawing</td>
</tr>
<tr>
<td>- Maximum insulation diameter: 4.40 mm [0.175 in] for Molex crimp lugs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Maximum insulation diameter: 5.8 mm [0.23 in] for Panduit crimp lugs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Red stranded wire to build the power cable based on the length required:</td>
<td>Length required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Maximum insulation diameter: 4.40 mm [0.175 in] for Molex crimp lugs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Maximum insulation diameter: 5.8 mm [0.23 in] for Panduit crimp lugs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hand crimp tool:</td>
<td>1</td>
<td>640010100 or equivalent</td>
<td>Molex product catalog</td>
</tr>
<tr>
<td>- Molex Premium Grade Hand Crimp Tool</td>
<td></td>
<td></td>
<td>Application tooling specification sheet</td>
</tr>
<tr>
<td>- Panduit Hand Crimp Tool</td>
<td></td>
<td>CT-460 or equivalent</td>
<td>Panduit product catalog</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application tooling specification sheet</td>
</tr>
</tbody>
</table>

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
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
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

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

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

Access procedure

To obtain the list of default user names and passwords, refer to Default user names and passwords.
Step_1  From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC. 
**NOTE:** The HTTPS prefix is mandatory. 
https://[BMC_MNGMT_IP]

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

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

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

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 parser command-line tool such as `jq` is installed.

### 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] |
| 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 parser 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] |
| 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 using IPMI over LAN (IOL)**

**Prerequisites**
The BMC IP address is known.

The remote computer has access to the management network subnet.

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.

<table>
<thead>
<tr>
<th>Step_1</th>
<th>From a remote computer that has access to the management network subnet, enter the desired command.</th>
</tr>
</thead>
</table>

**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**

<table>
<thead>
<tr>
<th>Step_1</th>
<th>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, enter the desired command.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LocalServer_OSPrompt:~# ipmitool [IPMI command]</td>
</tr>
</tbody>
</table>
Accessing the operating system of a server

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

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. But, 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

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

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

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

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

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

*NOTE: The HTTPS prefix is mandatory.*

https://[BMC MNGMT_IP]

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

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

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

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**

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

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

**Access procedure**

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

To obtain the list of default user names and passwords, refer to [Default user names and passwords](#).
Step 1: From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC.
   NOTE: The HTTPS prefix is mandatory.
   https://[BMC MNGMT_IP]

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

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

Step 4: Log in to the BMC Web UI using the appropriate credentials.

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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 to 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.

```
```

Step 2
Activate an SOL session.

```
```

Step 3
The OS start screen will be displayed.

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

Accessing an OS using 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 Location

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Physically connect a computer to the platform serial port.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Using a serial console tool, establish communication using the parameters provided. Press Enter.</td>
</tr>
<tr>
<td>Step_3</td>
<td>The OS start screen will be displayed.</td>
</tr>
</tbody>
</table>

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

Table of contents
- Accessing the UEFI or BIOS using Serial over LAN using the Web UI
  - Prerequisites
  - Browser considerations
  - Access procedure
- Accessing the UEFI or BIOS using the KVM
  - Prerequisites
  - Browser considerations
  - Access procedure
- Accessing the UEFI or BIOS using Serial over SSH
  - Prerequisites
  - Access procedure
- Accessing the UEFI or BIOS using Serial over LAN using IPMI
  - Prerequisites
  - Access procedure
- Accessing the UEFI or BIOS using a serial console through a physical connection
  - Prerequisites
  - Port location
  - Access procedure

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
- 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

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

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

Access procedure
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.

\[\text{NOTE: The HTTPS prefix is mandatory.}\]

\[https://[BMC\ MNGMT\_IP]\]

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

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

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

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**

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

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

**Access procedure**

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

**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 start the HTTPS self-signed certificate acceptance process. Information on the error message will be displayed.

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

**Step_4** Log in to the BMC Web UI using the appropriate credentials.
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.
Accessing the UEFI or BIOS using Serial over SSH

Prerequisites

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The BMC IP address is known.</td>
</tr>
<tr>
<td>2</td>
<td>The remote computer has access to the management network subnet.</td>
</tr>
<tr>
<td>3</td>
<td>An SSH client tool is installed on the remote computer.</td>
</tr>
</tbody>
</table>

**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
### 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](#).

---

**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.

![SSH Session](image)

**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...". Press 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.

![UEFI/BIOS Setup Menu](image)

---

**NOTE:** When a server reset command is sent, it may take a few seconds for the UEFI/BIOS sign on screen to display.
Step_1
From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session.

Step_2
Activate an SOL session.
NOTE: It may be required to press the Enter key for the operating system's screen to be displayed.

Step_3
From another command-line window. Make the platform enter the UEFI/BIOS automatically on the next reboot using the following command.

Step_4
From the same command-line window, perform a server 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 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
- Accessing the switch NOS using the Web UI
  - Prerequisites
  - Browser considerations
  - Access procedure
- Accessing the switch NOS CLI using the BMC Web UI Serial over LAN console
  - Prerequisites
  - Browser considerations
  - Access procedure
  - Accessing the BMC of the server for which you want to access the NOS
  - Launching the Web UI SOL console
- Accessing the switch NOS CLI using Serial over SSH from a remote computer
  - Prerequisites
  - Access procedure
- Accessing the switch NOS CLI using SSH from a remote computer
  - Prerequisites
  - Access procedure
- Accessing the switch NOS CLI using SSH from the integrated server
  - Prerequisites
  - Access procedure

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

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

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

Access procedure

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

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

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

Access procedure

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 start the HTTPS self-signed certificate acceptance process. Information on the error message will be displayed.  

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

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

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 to 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From a remote computer, open an SSH client tool and connect with the NOS IP address.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Log in the switch NOS CLI using the appropriate credentials.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Access the integrated server operating system using the preferred method.</td>
</tr>
</tbody>
</table>
| 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
  - Discovering the platform BMC IP address with DHCP Dynamic DNS update
    - Prerequisites
    - Procedure
  - Discovering the platform BMC IP address using the UEFI or BIOS
    - Prerequisites
    - Procedure
  - Discovering the BMC network configuration menu
- Discovering the switch NOS IP address
  - Discovering the switch NOS IP address with DHCP Dynamic DNS update
    - Prerequisites
    - Procedure
  - Discovering the switch NOS IP address through the switch NOS serial console CLI
    - Prerequisites
    - Procedure
  - Discovering the switch NOS IP address using DHCP server logs
    - Prerequisites
    - Procedure

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
RemoteComputer_DSPrompt--$ ping BMC00A0A5D2E90A

Discovering the platform BMC IP address using the UEFI or BIOS

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

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

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

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.

<table>
<thead>
<tr>
<th>IPMI and UEFI/BIOS</th>
<th>Redfish and Web UI</th>
<th>Network connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN channel 1</td>
<td>eth0</td>
<td>Front panel Srv 5</td>
</tr>
<tr>
<td>LAN channel 2</td>
<td>eth1</td>
<td>Internal server port 4 → switch port 16 *</td>
</tr>
</tbody>
</table>

* 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: DHCPCONFIG from 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPDISCOVER on 172.16.211.126 to 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPDISCOVER request from 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPACK on 172.16.211.126 to 00:a0:a5:d2:e9:0a via ens192
```

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:a0:a5:d2:e9:0a</td>
<td>MAC address discovered for the device (refer to section MAC addresses)</td>
</tr>
<tr>
<td>ens192</td>
<td>Linux DHCP server network interface name</td>
</tr>
<tr>
<td>172.16.211.126</td>
<td>IP address assigned to the device by the DHCP server</td>
</tr>
<tr>
<td>172.16.0.10</td>
<td>Linux DHCP server IP address</td>
</tr>
</tbody>
</table>

**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**

```
Step 1: Ping the host name.
RemoteComputer_DSPROMPT--$ 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 to 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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Access to the DHCP server logs is required.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>The first assigned MAC address of the switch NOS is known.</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:a0:a5:d2:e9:0a</td>
<td>MAC address discovered for the device (refer to section MAC addresses)</td>
</tr>
<tr>
<td>ens192</td>
<td>Linux DHCP server network interface name</td>
</tr>
<tr>
<td>172.16.211.126</td>
<td>IP address assigned to the device by the DHCP server</td>
</tr>
<tr>
<td>172.16.0.10</td>
<td>Linux DHCP server IP address</td>
</tr>
</tbody>
</table>
Default user names and passwords

Table of contents
- Management interface (BMC)
- Switch network operating system (NOS)
- Operating system
- UEFI/BIOS

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.

<table>
<thead>
<tr>
<th>User name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>ready2go</td>
</tr>
</tbody>
</table>

Switch network operating system (NOS)

<table>
<thead>
<tr>
<th>User name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>ready2go</td>
</tr>
</tbody>
</table>

Operating system

The user name and password are application-specific. However, if Kontron provided an operating system, the credentials will be the following:

<table>
<thead>
<tr>
<th>User name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>kontron</td>
</tr>
</tbody>
</table>

UEFI/BIOS

No default password is set.
Software installation and deployment
## Preparing for operating system installation

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose the operating system needed based on the requirements of your application. It is recommended to choose one from the list of validated operating systems.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Confirm the OS version to be installed includes or has drivers supporting the platform components listed in the PCI mapping.</td>
</tr>
<tr>
<td>Step 3</td>
<td>If applicable, download the ISO file of the OS to be installed.</td>
</tr>
</tbody>
</table>

For a list of known compatible operating systems, refer to [Validated operating systems](#).

For information on components, refer to the [PCI mapping](#).
Installing an operating system on a server

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

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.

![KVM launch](image)

Step_2 A new browser window opens and displays the virtual server screen.

![KVM virtual server](image)

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
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a bootable USB key using the appropriate software. <strong>NOTE:</strong> RUFUS is recommended.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Insert the USB key into one of the USB ports of the front panel.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Power on the platform and access the UEFI/BIOS setup menu.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Navigate to the <strong>Save &amp; Exit</strong> menu and then to the <strong>Boot Override</strong> section.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose the USB option desired.</td>
</tr>
</tbody>
</table>
Verifying operating system installation

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.

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.

<table>
<thead>
<tr>
<th>Step_10</th>
<th>(Optional) If one or two PCIe add-in cards are installed, verify that the cards are detected.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>LocalServer_OSPrompt:~# lspci</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_11</th>
<th>Verify communication between the operating system and the BMC.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>LocalServer_OSPrompt:~# ipmitool mc info</code></td>
</tr>
</tbody>
</table>

**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

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

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

Script example

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

```c
#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+.

Version 1.0 (March 2023)

www.kontron.com

// 120


Additional low level information
The information in this 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.

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Address offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp PCIe 1 mbox</td>
<td>0xA28</td>
</tr>
<tr>
<td>Temp PCIe 2 mbox</td>
<td>0xA29</td>
</tr>
</tbody>
</table>

Converting a temperature to hexadecimal
Positive values are represented by hexadecimal numbers from 0x00 to 0x7F.
- O°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 0x81.
- -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.

```bash
```

Adding a virtual FRU

Step_1 Add a PCIe card to the virtual FRU using the following command.

```bash
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
```

Step_2 Reboot the BMC to apply the changes.

```bash
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
```

Version 1.0 (March 2023)
Removing a virtual FRU

Step_1 To unregister a PCIe add-in card from the virtual FRU, use the following command.

```bash
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.

```bash
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
```

Version 1.0 (March 2023) www.kontron.com // 122
Common software installation

Table of contents
- Required software tools
- Recommended software tools

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

Required software tools

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

Recommended software tools

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

Table of contents
- Privilege levels
- Configuring user names and passwords
  - Using the Web UI
  - Using Redfish
  - Using IPMI
- Adding a user
  - Using the Web UI
  - Using Redfish
  - Using IPMI
- Deleting a user
  - Using the Web UI
  - Using Redfish
  - Using IPMI
- Configuring privilege level
  - Using the Web UI
  - Using Redfish
  - Using IPMI

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

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

<table>
<thead>
<tr>
<th>Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>0x4 - Administrator. Users are allowed to configure everything regarding the BMC (including user management and network configuration). Users will have full administrative access.</td>
</tr>
<tr>
<td>Operator</td>
<td>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.</td>
</tr>
<tr>
<td>User</td>
<td>0x1 - Callback. Users only have read access and can't change any behavior of the system. Users can change their own passwords.</td>
</tr>
<tr>
<td>No-Access</td>
<td>0xF - No Access. Users with this privilege level will not have access to the BMC.</td>
</tr>
</tbody>
</table>

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 Save.

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

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

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 IDL. 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.
<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the left-side menu, click on <strong>Security and access</strong> and then on <strong>User management</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Click on <strong>Add user</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Fill the required fields and click on <strong>Add user</strong>.</td>
</tr>
</tbody>
</table>

**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

| curl -k s --request GET --url https://[SERVER_IP]/redfish/v1/AccountService/Roles | jq |
|---|
| "odata.id": /redfish/v1/AccountService/Roles/Administrator, |
| "odata.id": /redfish/v1/AccountService/Roles/Operator, |
| "odata.id": /redfish/v1/AccountService/Roles/ReadOnly, |
| "odata.id": /redfish/v1/AccountService/Roles/NoAccess |

### 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

$ curl -k s --request POST --url https://[SERVER_IP]/redfish/v1/AccountService/Accounts --header 'Content-Type: application/json' --data "{"Password": "[PASSWORD]", "RoleId": "[ROLE_ID]", "UserName": "[USER_NAME]"}" | jq

<table>
<thead>
<tr>
<th>Message.ExtendedInfo:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;MessageId&quot;: &quot;ipmitool.SetFailedGenericError&quot;,</td>
</tr>
<tr>
<td>&quot;Message&quot;: &quot;The resource has been created successfully&quot;,</td>
</tr>
<tr>
<td>&quot;MessageArgs&quot;: [],</td>
</tr>
<tr>
<td>&quot;MessageKey&quot;: &quot;None&quot;,</td>
</tr>
<tr>
<td>&quot;Resolution&quot;: &quot;None&quot;</td>
</tr>
</tbody>
</table>

### 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 IDL. To use IDL, add the IDL 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 list of users and select the ID of the user to add.

LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]

#### Step 2
Create a user name.

LocalServer_OSPrompt:~# ipmitool user set name [IPMI user ID] [new IPMI user name]

**NOTE:** The first and second user names of the user list are reserved fields and therefore can't be modified.

#### Step 3
Create the password.

LocalServer_OSPrompt:~# ipmitool user set password [IPMI user ID] [new IPMI password]

#### Step 4
Enable channel access and configure privilege level.

LocalServer_OSPrompt:~# ipmitool channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]

#### Step 5
Enable the user.

LocalServer_OSPrompt:~# ipmitool user enable [USER_ID]

### Deleting 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 be 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 fields 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' -d '"RoleId": [ROLE]' | jq

### 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.

---

### 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 IDL. To use IDL, add the IDL 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 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]
Configuring and managing switch NOS users

Table of contents

- Configuring switch NOS users using the switch NOS Web UI
  - Changing the password of a user
  - Adding a user
  - Deleting a user
  - Configuring privilege level
- Configuring switch NOS users using the switch NOS CLI
  - Changing the password of a user
  - Adding a user
  - Deleting a user
  - Configuring privilege level

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-->(config-if)# **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](#).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From the left-side menu, select <strong>Configuration &gt; Security &gt; Switch</strong> and then <strong>Users</strong>.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Click on the desired user.</td>
</tr>
<tr>
<td>Step_3</td>
<td>Change the value of the <strong>Change Password</strong> dropdown menu to <strong>Yes</strong>.</td>
</tr>
<tr>
<td>Step_4</td>
<td>Enter the password in fields <strong>Password</strong> and <strong>Password (again)</strong>.</td>
</tr>
<tr>
<td>Step_5</td>
<td>Click on <strong>Save</strong> to confirm.</td>
</tr>
<tr>
<td>Step_6</td>
<td>(Optional) To make the change persistent, save running-config to startup-config.</td>
</tr>
</tbody>
</table>

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](#).
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the left-side menu, select Configuration, Security, Switch and then Users.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click on the Add New User button.</td>
</tr>
</tbody>
</table>
| **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](#).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the left-side menu, select Configuration, Security, Switch and then Users.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click on the desired user.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click on the Delete User button.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>The user should be removed from the user list.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) To make the change persistent, save running-config to startup-config.</td>
</tr>
</tbody>
</table>

**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](#).
### 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](#).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step_1 | Access the configuration setup menu.  
LocalSwitchNOS_OSPrompt:~# configure terminal |
| Step_2 | Change the password.  
LocalSwitchNOS_OSPrompt:~(config)# username [USERNAME] privilege [PRIVILEGE_LEVEL] password unencrypted [NEW_PASSWORD] |
| 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](#).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step_1 | Access the configuration setup menu.  
LocalSwitchNOS_OSPrompt:~# 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] |
| 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](#).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step_1 | Access the configuration setup menu.  
LocalSwitchNOS_OSPrompt:~# configure terminal |
| Step_2 | Delete the user.  
LocalSwitchNOS_OSPrompt:~(config)# no username [USERNAME] |
| 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](#).
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command/Example</th>
</tr>
</thead>
</table>
| Step 1| Access the configuration setup menu.                                        | LocalSwitchNOS_OSPrompt:~
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] |
| Step 3| (Optional) To make the change persistent, save running-config to startup-config. | (config)# username user privilege 11 password unencrypted Password |
Configuring date and time
Configuring BMC date and time

Table of contents
- General information on platform date and time
- Configuring the BMC date and time
  - Configuring the BMC date and time using the Web UI
    - Manually configuring the BMC date and time using the Web UI
    - Configuring the BMC date and time based on the NTP using the Web UI
  - Configuring the BMC date and time using Redfish
    - Manually configuring the BMC date and time using Redfish
    - Configuring the BMC date and time based on the NTP using Redfish
  - Configuring the BMC date and time using IPMI
    - Manually configuring the BMC date and time using IPMI

General information on platform date and time

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

Configuring the BMC date and time

The BMC date and time can be set using:
- The BMC Web UI
- Redfish
- IPMI

Configuring the BMC date and time using the Web UI

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

Manually configuring the BMC date and time using the Web UI

Step_1
From the left-side menu, select Settings and then Date and time.

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 configuring the BMC date and time using Redfish**

**Step 1**
If NTP is enabled, disable it.


**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

**Step 3**
Verify BMC current date and time.

RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc | jq .DateTime

**Configuring the BMC date and time based on the NTP using Redfish**
Step_1 | Add the NTP server(s) and enable the protocol. 

Step_2 | Verify BMC current date and time. 
RemoteComputer_OSPrompt:~$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc | jq .DateTime

### Configuring the BMC date and time using IPMI

It is only possible to set time manually using IPMI.

**Manually configuring the BMC date and time using IPMI**

The following procedures will be executed using the Accessing a BMC using IPMI 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]"

**Step_2** Verify that the system event log time was properly set. 
LocalServer_OSPrompt:~# ipmitool sel time get

### Known limitation

**Problem**

When setting the system event log time with `ipmitool`, multiple repeated System Event entries will be present in the SEL list.

**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 time set. 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
- Configuring the switch NOS date and time source based on the NTP
  - Configuring the switch NOS date and time source based on the NTP using the Web UI
  - Configuring the switch NOS date and time source based on the NTP using the CLI
- Configuring the switch NOS date and time source based on the PTP
  - Configuring the switch NOS date and time zone and daylight saving time
    - Configuring the switch NOS date and time zone and daylight saving time using the Web UI
    - Configuring the switch NOS date and time zone and daylight saving time using the CLI

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

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

Step_2 Enable the NTP.
LocalSwitchNOS_OSPrompt:~(config)# ntp
NOTE: To disable NTP, use no 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.

Step_4 Exit configuration mode.
LocalSwitchNOS_OSPrompt:~(config)# exit

Step_5 Verify the NTP configuration by displaying the list of NTP servers.
LocalSwitchNOS_OSPrompt:~# show ntp status

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] [STARTING_HH:MM] [ENDING_WEEK] [ENDING_MONTH] [ENDING_DAY] [ENDING_HH:MM] [OFFSET]
NOTE: This command sets the parameters for every year. No reprogramming needed.

Step_4 Verify the time zone configuration.
LocalSwitchNOS_OSPrompt:~(config)# exit
LocalSwitchNOS_OSPrompt:~# show clock detail

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

Table of contents
- Selecting an access method for BMC networking configuration
- BMC network architecture
  - Ethernet switch IO module option
  - Pass-through IO module option
- Enabling or disabling a BMC network interface
  - Enabling or disabling a BMC network interface using Redfish
  - Enabling or disabling a BMC network interface using the BMC Web UI
  - Enabling or disabling a BMC network interface using IPMI
- Configuring a static IP address
  - Configuring a static IP address using Redfish
  - Configuring a static IP address using the BMC Web UI
  - Configuring a static IP address using the UEFI/BIOS setup menu
  - Configuring a static IP address using IPMI
- Configuring a dynamic IP address using DHCP
  - Configuring a dynamic IP address using Redfish
  - Configuring a dynamic IP address using the BMC Web UI
  - Configuring a dynamic IP address using the UEFI/BIOS setup menu
  - Configuring a dynamic IP address using IPMI
- Configuring a VLAN for a BMC network interface
  - Assigning a VLAN
    - Assigning a VLAN using Redfish
    - Assigning a VLAN using the BMC Web UI
    - Assigning a VLAN using IPMI
  - Removing a VLAN
    - Removing a VLAN using Redfish
    - Removing a VLAN using the BMC Web UI
    - Removing a VLAN using IPMI
- Configuring the integrated server Redfish host interface IP address

To configure the BMC networking IP address, a schema must be selected and configured:
- A static IP address
- A dynamic IP address using DHCP

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

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

Relevant sections:
- 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
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.

<table>
<thead>
<tr>
<th>IPMI and UEFI/BIOS</th>
<th>Redfish and Web UI</th>
<th>Network connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN channel 1</td>
<td>eth0</td>
<td>Front panel Srv 5</td>
</tr>
<tr>
<td>LAN channel 2</td>
<td>eth1</td>
<td>Internal server port 4 → switch port 16 *</td>
</tr>
</tbody>
</table>

* 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.

**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

```
[ { "Id" : "redfish/v1/Managers/bmc/EthernetInterfaces", "Name" : "Collection of EthernetInterfaces for this Manager", "Members@odata.count" : 2, "@odata.id" : "/redfish/v1/Managers/bmc/EthernetInterfaces/eth0", "Members@odata.id" : "/redfish/v1/Managers/bmc/EthernetInterfaces/eth0" }, { "Id" : "redfish/v1/Managers/bmc/EthernetInterfaces/eth1", "Name" : "Ethernet Network Interface Collection" } ]
```

**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

```
[ { "Id" : "redfish/v1/Managers/bmc/EthernetInterfaces/eth0", "Name" : "Ethernet Network Interface Collection" } ]
```

**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 IDL. To use IDL, add the IDL parameters to the command: `-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": ["IP_ADDRESS","MASK","GATEWAY"]}}' | 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 the Server Mgmt tab.

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
**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**
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 the 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]
```

---

Version 1.0 (March 2023) www.kontron.com // 153
### 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. The 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 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.

<table>
<thead>
<tr>
<th>Step_1</th>
<th>Select a BMC network interface and take note of its URL.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteComputer_OSPrompt:~#</td>
<td>curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces</td>
</tr>
</tbody>
</table>

```bash
$ curl -k -s --request GET --url https://admin-readygpo172.14.182.31/redfish/v1/Managers/bmc/EthernetInterfaces | jq
```

```json

```

<table>
<thead>
<tr>
<th>Step_2</th>
<th>Add a VLAN for the selected BMC network interface using the following command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteComputer_OSPrompt:~#</td>
<td>curl -k -s --request POST --url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]/VLANs --header 'Content-Type: application/json' --data '{&quot;VLANEnable&quot;: true,&quot;VLANId&quot;: [VLAN_ID]} '</td>
</tr>
</tbody>
</table>

```bash
$ curl -k -s --request POST --url https://admin-readygpo172.14.182.31/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]/VLANs --header 'Content-Type: application/json' --data '{"VLANEnable": true,"VLANId": [VLAN_ID]} ' | jq
```

```json

```

| Step_3 | Configure an IP address for the VLAN interface created using one of the Redfish methods described in this section. |

Assigning a VLAN using the BMC Web UI

Refer to Accessing a BMC using the Web UI for access instructions.
**Step 1**  From the left-side menu of the BMC Web UI, select **Settings** and then **Network**.

**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 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**  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**
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.

```bash
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.

```bash
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.

```bash
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.

```bash
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.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From the left-side menu of the BMC Web UI, select Settings and then Network.</td>
</tr>
<tr>
<td>Step_2</td>
<td>From the dropdown menu of the Interface section, select a network interface to configure.</td>
</tr>
<tr>
<td>Step_3</td>
<td>To remove a VLAN, uncheck the box in the VLAN section.</td>
</tr>
<tr>
<td>Step_4</td>
<td>Click on Save settings.</td>
</tr>
</tbody>
</table>

### 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:

```
```

**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:
```
In this example the interface name discovered is enp0s20f0u3u2.
```

Example in Ubuntu:
```
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]

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]
Configuring UEFI network boot

Table of contents
- Configuring UEFI network boot using the UEFI/BIOS menu
  - Prerequisites
  - Configuring UEFI networking using the UEFI/BIOS menu
    - Identifying the network interfaces
    - Enabling UEFI support for installed network controllers
  - Configuring PXE network boot using the UEFI/BIOS menu
    - Enabling PXE support
    - Performing PXE network boot
  - Configuring HTTP network boot using the UEFI/BIOS menu
    - Enabling HTTP boot support
    - Performing HTTP network boot
  - Configuring VLANs for UEFI network boot using the UEFI
    - Creating VLANs
    - Removing VLANs

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

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access to the UEFI/BIOS menu is required.</td>
</tr>
</tbody>
</table>
| 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 10GbE 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.

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

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 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 I/O module, VLANs must be configured for any VLAN-tagged traffic coming from the server E823 10GbE interface. Refer to Configuring the switch for procedures to configure VLANs with the switch network operating system.

The UEFI/BIOS setup menu provides options to create/configure/remove VLANs on each of the server’s four E823 NIC 10GbE 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 10GbE 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 10GbE 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 of the E823 10GbE 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 10GbE interface, as needed.

Step_4  Press F4 to save changes and exit.
Configuring switch NOS networking

Table of contents
- Configuring IP addresses to access the switch NOS
  - Adding a NOS VLAN interface IP address
    - Adding a NOS VLAN interface IP address using the Web UI
      - Adding a NOS VLAN interface
      - Configuring a static IP address
      - Configuring a dynamic IP address using DHCP
    - Adding a NOS VLAN interface IP address using the CLI
      - Adding a NOS VLAN interface using a static IP address
      - Adding a NOS VLAN interface using DHCP
  - Removing a NOS VLAN interface IP address
    - Removing a NOS VLAN interface IP address using the Web UI
    - Removing a NOS VLAN interface IP address using the CLI
  - Configuring HTTPS support
    - Configuring HTTPS support using the Web UI
      - HTTPS configuration page
        - Values available for fields used for HTTPS configuration
        - Certificates
          - Generating a self-signed certificate
          - Uploading a certificate from a URL
          - Uploading a certificate from a user file system
          - Deleting an installed certificate
      - Configuring the interface protocol
        - Configuring the interface for HTTP only
        - Configuring the interface for HTTPS only
        - Configuring the interface for HTTP and HTTPS
    - Configuring HTTPS support using the CLI
      - Displaying HTTP and HTTPS states
      - Certificates
        - Displaying available commands
        - Generating a self-signed certificate
        - Uploading a certificate from a URL
        - Deleting an installed certificate
      - Configuring the interface protocol
        - Configuring the interface for HTTP only
        - Configuring the interface for HTTPS only
        - Configuring the interface for HTTP and HTTPS
  - Configuring DNS
    - Configuring the domain name
      - Configuring the domain name using the CLI
      - Configuring the domain name using the Web UI
    - Configuring a DNS server
      - Configuring a DNS server using the CLI
      - Configuring a DNS server using the Web UI
    - Configuring proxy DNS
      - Configuring proxy DNS using the CLI
      - Enabling proxy DNS using the Web UI

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]
```

**Step 2** Set the static IP address source.

```
LocalSwitchNOS_OSPrompt:(config-if-vlan)# ip address [IP_ADDRESS] [MASK]
```

**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]
```

**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`.

**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.

Version 1.0 (March 2023)
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
```

Step_2: Remove the VLAN.
```
LocalSwitchNOS_OSPrompt:~(config)# no interface vlan [VLAN_ID]
```

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.

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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Sets the HTTPS operation mode.</td>
<td><em>Enabled</em>: HTTPS operation mode is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Disabled</em>: HTTPS operation mode is disabled.</td>
</tr>
<tr>
<td><strong>Automatic Redirect</strong></td>
<td>Sets the HTTPS redirect operation mode.</td>
<td><em>Enabled</em>: HTTPS redirect operation mode is enabled.</td>
</tr>
<tr>
<td></td>
<td>This setting is required only when <strong>Mode</strong> is set to <strong>Enabled</strong>.</td>
<td><em>Disabled</em>: HTTPS redirect operation mode is disabled.</td>
</tr>
<tr>
<td></td>
<td>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 <strong>Enabled</strong>, the HTTP protocol is effectively disabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Certificate Maintain</strong></td>
<td>Performs certificate maintenance. This setting is operational only when <strong>Mode</strong> is set to <strong>Disabled</strong>.</td>
<td><em>None</em>: Nothing happens.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Delete</em>: Deletes the current certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Upload</em>: Uploads a certificate PEM file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Generate</em>: Generates a new self-signed RSA certificate.</td>
</tr>
<tr>
<td><strong>Certificate Pass Phrase</strong> (Available when the <strong>Certificate Maintain</strong> field is set to <strong>Upload</strong>.)</td>
<td>Holds the passphrase protecting the certificate to upload.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>URL</em>: Upload a certificate via an URL.</td>
</tr>
</tbody>
</table>

---

Version 1.0 (March 2023)  www.kontron.com
when the Certificate Maintain field is set to Upload.

The file should contain both the certificate and private key. If the certificate and private key are in 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).

<table>
<thead>
<tr>
<th><strong>File Upload</strong> (Available when the Certificate Upload field is set to Web Browser)</th>
<th>Lets users select the file to upload.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong> (Available when the Certificate Upload field is set to URL)</td>
<td>Holds the URL.</td>
</tr>
</tbody>
</table>
| 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. |

<table>
<thead>
<tr>
<th><strong>Certificate Status</strong></th>
<th>Displays the current status of the switch certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch secure HTTP certificate is presented</strong></td>
<td>When a valid certificate is present.</td>
</tr>
<tr>
<td><strong>Switch secure HTTP certificate is not presented</strong></td>
<td>When no valid certificate is present or the certificate has been deleted.</td>
</tr>
<tr>
<td><strong>Switch secure HTTP certificate is generating ...</strong></td>
<td>When the self-signed certificate is being generated (wait 1 minute and then refresh the page for results).</td>
</tr>
</tbody>
</table>

**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 through a chain of trust. 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 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.

There 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).

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

**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 trust. 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

**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.

Your connection is not private

Advisors might be trying to steal your information from HTTP(S), for example, passwords, messages, or credit card authorization.

To get Chrome's highest level of security, turn on enhanced protection

This server could not prove that it is [IP_ADDRESS] & its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connections.

Proceed to [IP_ADDRESS] (unsafe)

From the network switch CLI:

**Step 1** Go in configuration mode.
LocalSwitchNOS_OSPrompt:~# configure terminal

**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.

**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]

**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.

**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

**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:
### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enter the configuration terminal.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>no ip http secure-server</code></td>
</tr>
<tr>
<td>Step 3</td>
<td>Ensure the certificate and HTTP web server are correctly configured.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) To make the change persistent, save running-config to startup-config.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enter the configuration terminal.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip http secure-server</code></td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable redirection.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Ensure the certificate and HTTP web server are correctly configured.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) To make the change persistent, save running-config to startup-config.</td>
</tr>
</tbody>
</table>

### Configuring the interface for HTTP and HTTPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enter the configuration terminal.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip http secure-server</code></td>
</tr>
<tr>
<td>Step 3</td>
<td>Ensure the certificate and HTTP web server are correctly configured.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) To make the change persistent, save running-config to startup-config.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Verify that configuration was successful.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) To make the change persistent, save running-config to startup-config.</td>
</tr>
</tbody>
</table>
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
```

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.

- To set the DNS server ID, use the `name-server [DNS_SERVER_ID]` command.
- To configure a DNS server from a specific DHCPv4-enabled VLAN interface, use the `name-server dhcp ipv4 interface vlan [VLAN_ID]` command.
- To disable a DNS server, use the `no` prefix before the `name-server` command.

```
LocalSwitchNOS_OSPrompt:~# name-server 10.232.30.5
LocalSwitchNOS_OSPrompt:~# name-server 10.232.30.6 dhcp ipv4
LocalSwitchNOS_OSPrompt:~# name-server 10.232.30.7 dhcp ipv4 interface vlan 1

LocalSwitchNOS_OSPrompt:~# do name-server
```

Step_3  Verify that configuration was successful.

```
LocalSwitchNOS_OSPrompt:~# do show ip name-server
```

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, select the DNS server 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 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
```

**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
```

**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
  - Configuring SNMP remote management using the BMC Web UI
  - Configuring SNMP remote management using Redfish

## 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From the left-side menu, select <strong>Security and access</strong> and then <strong>Policies</strong>.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Enable or disable SNMP remote management using the radio button.</td>
</tr>
<tr>
<td>Step_3</td>
<td>If SNMP remote management was enabled, change the Community String to a unique name.</td>
</tr>
<tr>
<td>Step_4</td>
<td>Click on the <strong>Save</strong> button.</td>
</tr>
<tr>
<td>Step_5</td>
<td>A success message should appear upon successful configuration.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step_1 | Enable or Disable SNMP remote management using the following command. Possible values for [ENABLED] are:  
  - true  
  - false  
  ```bash  
  curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Managers/bmc/NetworkProtocol --header 'Content-Type: application/json' --data '{"SNMP":{"ProtocolEnabled":['ENABLED']}}' | jq  
  ``` |
| Step_2 | Configure SNMP remote management **Community String**. Ensure that [STRING] is a unique community name.  
  ```bash  
  ``` |
Configuring BMC event subscriptions

Table of contents
- Configuring the SNMP traps
  - Configuring the SNMP traps using the BMC Web UI
  - Configuring the SNMP traps using Redfish

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_0SPrompt:~$ 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

```json
{
  "Message.ExtendedInfo": [
    {
      "MessageId": "Message.v1_1.1.Message",
      "Message": "The resource has been created successfully",
      "MessageSeverity": "OK",
      "Resolution": "None"
    }
  ]
}
```

Version 1.0 (March 2023)
# Configuring the switch

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

## 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.
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 \([\text{INTERFACE}_\text{ID}]\) 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.

<table>
<thead>
<tr>
<th>NOS port designation</th>
<th>Connection device</th>
<th>Integrated server PCIe bus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 1/1</td>
<td>SFP Sw 1</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/2</td>
<td>SFP Sw 2</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/3</td>
<td>SFP Sw 3</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/4</td>
<td>SFP Sw 4</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/5</td>
<td>SFP Sw 5</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/6</td>
<td>SFP Sw 6</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/7</td>
<td>SFP Sw 7</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/8</td>
<td>SFP Sw 8</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/9</td>
<td>SFP Sw 9</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/10</td>
<td>SFP Sw 10</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/11</td>
<td>SFP Sw 11</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/12</td>
<td>SFP Sw 12</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet 1/13</td>
<td>eno1 *</td>
<td>00:89:00.3</td>
</tr>
<tr>
<td>Ethernet 1/14</td>
<td>eno2 *</td>
<td>00:89:00.2</td>
</tr>
<tr>
<td>Ethernet 1/15</td>
<td>eno3 *</td>
<td>00:89:00.1</td>
</tr>
<tr>
<td>Ethernet 1/16</td>
<td>eno4 *</td>
<td>00:89:00.0</td>
</tr>
</tbody>
</table>

* 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

<table>
<thead>
<tr>
<th>Port map</th>
<th>Active front panel SFP ports</th>
<th>Internal server ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>12x SFP+ 10GbE</td>
<td>SFP1-12</td>
</tr>
<tr>
<td>1</td>
<td>7x SFP+ 10GbE 2x SFP28 25GbE</td>
<td>SFP1-7 SFP9-10</td>
</tr>
<tr>
<td>2</td>
<td>2x SFP+ 10GbE 4x SFP28 25GbE</td>
<td>SFP1-2 SFP9-12</td>
</tr>
<tr>
<td>3</td>
<td>4x SFP28 25GbE</td>
<td>SFP9-12</td>
</tr>
</tbody>
</table>

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.

Version 1.0 (March 2023) www.kontron.com // 190
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

<table>
<thead>
<tr>
<th>ID</th>
<th>10Gb ports</th>
<th>25Gb ports</th>
<th>Unused ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1/1-16</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>1</td>
<td>1/1-13-16</td>
<td>1/9-10</td>
<td>1/8-12-14-16</td>
</tr>
<tr>
<td>2</td>
<td>1/1-13-16</td>
<td>1/9-12</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>None</td>
<td>1/9-16</td>
<td></td>
</tr>
</tbody>
</table>
|    |            |            | Active port map configuration: 0

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.

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:

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]

Switch must be rebooted for new port map to take effect

NOTE: The ID is the value of parameter [PORTMAP_ID] used in the commands.

Step 3: Exit configuration mode and reboot the switch NOS to make the new configuration effective.
LocalSwitchNOS_OSPrompt:~(config)# end
LocalSwitchNOS_OSPrompt:~# reload cold

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Speed</th>
<th>Duplex</th>
<th>Status</th>
<th>Media Type</th>
<th>SFP Family</th>
<th>Link</th>
<th>Operational Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>Enabled</td>
<td>Auto</td>
<td>10G</td>
<td>No</td>
<td>SFP</td>
<td>SFP</td>
<td>10G optical</td>
<td>Down</td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>Enabled</td>
<td>Auto</td>
<td>10G</td>
<td>No</td>
<td>SFP</td>
<td>SFP</td>
<td>10G optical</td>
<td>Down</td>
</tr>
<tr>
<td>Eth 1/3</td>
<td>Enabled</td>
<td>Auto</td>
<td>10G</td>
<td>No</td>
<td>SFP</td>
<td>SFP</td>
<td>10G optical</td>
<td>Down</td>
</tr>
<tr>
<td>Eth 1/4</td>
<td>Enabled</td>
<td>Auto</td>
<td>10G</td>
<td>No</td>
<td>SFP</td>
<td>SFP</td>
<td>10G optical</td>
<td>Down</td>
</tr>
</tbody>
</table>

Version 1.0 (March 2023)
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]
```

**Step 2**

Enable the interface.

```
LocalSwitchNOS_OSPrompt:~(config-if)# no shutdown
```

**Step 3**

(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]
```

**Step 2**

Enable the interface.

```
LocalSwitchNOS_OSPrompt:~(config-if)# no shutdown
```

**Step 3**

(Optional) To make the change persistent, save running-config to startup-config.
### Step 1
Access the interface setup menu.
```
LocalSwitchNOS_OSPrompt:~# configure terminal
LocalSwitchNOS_OSPrompt:(config)# interface [INTERFACE_ID]
```

### Step 2
Disable the interface.
```
LocalSwitchNOS_OSPrompt:(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
```

### Step 2
Enter the interface configuration menu.
```
LocalSwitchNOS_OSPrompt:(config)# interface [INTERFACE]
```

### Step 3
Change the speed.
```
LocalSwitchNOS_OSPrompt:(config-if)# speed [SPEED]
```

### 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.

```
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Display the VLAN status for every switch port.</td>
</tr>
<tr>
<td></td>
<td>LocalSwitchNOS_OS&gt;show vlan</td>
</tr>
</tbody>
</table>
```

Displaying VLANs using the Web UI

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

```
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From the left-side menu, select Monitor, VLANs and then Membership. The VLAN port membership should be displayed.</td>
</tr>
</tbody>
</table>
```

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.

```
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td></td>
<td>LocalSwitchNOS_OS#configure terminal</td>
</tr>
<tr>
<td>Step_2</td>
<td>Create a new VLAN.</td>
</tr>
<tr>
<td></td>
<td>LocalSwitchNOS_OS(config)#vlan [VLAN_ID]</td>
</tr>
<tr>
<td>Step_3</td>
<td>(Optional) To make the change persistent, save running-config to startup-config.</td>
</tr>
</tbody>
</table>
```

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`

Step 2 Remove a VLAN using the following command.

`LocalSwitchNOS_OSPrompt:~(config)# no vlan [VLAN_ID]`

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]

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]

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`

Step 2  Configure static routing.
`LocalSwitchNOS_OSPrompt:~(config)# ip route [HOST_ADDRESS] [NETWORK_MASK] [GATEWAY_ADDRESS]`

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`

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.

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

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

Step 1: Restore the default configuration.
LocalSwitchNOS_OSPrompt:~# reload defaults

Step 2: To make the revert to default values permanent, use the following command.
LocalSwitchNOS_OSPrompt:~# copy running-config 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.
### 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
- Integrated GNSS receiver
  - Factory configuration
  - Configuring the antenna cable delay
- PTP based on IEEE 1588
  - PPS output
  - Switch NOS PTP External Clock Mode configuration
- Configuring the switch as a telecom grandmaster as per ITU-T G.8275.1
  - Prerequisite
  - Procedure
- Configuring the switch as a telecom boundary clock as per ITU-T G.8275.1
  - Prerequisite
  - Procedure
- Configuring the internal server as a telecom time slave clock as per ITU-T G.8275.1
  - Synchronizing the E823 PTP hardware clock
    - Prerequisite
    - Procedure
- Configuring synchronous Ethernet
  - Prerequisite
  - Procedure

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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default value</th>
<th>Value in this platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG-NAVSPG-DYNMODEL</td>
<td>Dynamic platform model</td>
<td>0 (Portable)</td>
<td>2 (Stationary)</td>
</tr>
<tr>
<td>CFG-UART1-BAUDRATE</td>
<td>Baud rate for UART1</td>
<td>38400</td>
<td>115200</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default value</th>
<th>Value in this platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG-TP-ANT_CABLEDELAY</td>
<td>Antenna cable delay</td>
<td>50 ns</td>
<td>User-defined</td>
</tr>
</tbody>
</table>

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](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.

1. From the UEFI/BIOS setup menu, navigate to the **Platform Configuration** tab and select **PCH Configuration**.

2. Select **USB Configuration**.

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
```

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.

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.

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 sole configurable parameter is the clock adjustment method. The default setting of "auto" is equivalent to "common" for IEEE1588 and G.8275.1 profiles. The available methods 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**: The 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 instance 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.

### Creating a switch NOS PTP instance

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

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

The switch can be configured as a telecom grandmaster (T-GM) (primary reference clock) using the switch NOS CLI or Web UI. The following 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**

Version 1.0 (March 2023)  
www.kontron.com  
// 202
To obtain meaningful results, the integrated GNSS receiver must acquire timing information. An appropriate antenna must be connected to the chassis GNSS input. Please refer to 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
```

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.

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
LocalSwitchNOS_Prompt(config)# time-property utc-offset 37 valid time-traceable
LocalSwitchNOS_Prompt(config)# freq-traceable ptptimescale time-source 32
LocalSwitchNOS_Prompt(config)# ptp 0 virtual-port class 6
LocalSwitchNOS_Prompt(config)# ptp 0 virtual-port accuracy 33
LocalSwitchNOS_Prompt(config)# ptp 0 virtual-port variance 20061
```

**NOTE:** The utc-offset value changes in time and should be chosen according to the current value.

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`.

Step 5 Add interfaces to the PTP instance.
```
LocalSwitchNOS_Prompt(config)# interface Ethernet 1/1,9,12
LocalSwitchNOS_Prompt(config-if)# ptp 0
```

Step 6 End configuration.
```
LocalSwitchNOS_Prompt(config-if)# end
```

Step 7 (Optional) To make the change persistent, save running-config to startup-config.
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
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
Version 1.0 (March 2023) www.kontron.com // 204
The switch can be configured as a telecom boundary clock (T-BC) using the switch NOS CLI or Web UI.

---

**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

**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.

**Step 3** (Optional) Set the NOS system time from the PTP instance.

LocalSwitchNOS_OSPrompt(config)# 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`.

**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

**Step 5** End configuration.

LocalSwitchNOS_OSPrompt(config-if)# end

**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.

**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.

**Version 1.0 (March 2023)**

www.kontron.com
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.

### 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.

**Procedure**

Log in to the server. Refer to [Accessing the operating system of a server](#) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Make sure the network interface is up.  
Server_OSPrompt:~# ifconfig eno1 up |
| 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]  
| 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.

**Procedure**

Log in to the server. Refer to [Accessing the operating system of a server](#) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Verify the running ptp4l status.  
Server_OSPrompt:~# ./linuxptp/pmc -u -d24 'GET CURRENT_DATA_SET' |
| 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**

**Version 1.0 (March 2023)**

www.kontron.com

// 207
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

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

Step_3 End configuration.
LocalSwitchNOS_OSPrompt(config-if)# end

Step_4 Verify the port status.
LocalSwitchNOS_OSPrompt# show network-clock

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

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

Version 1.0 (March 2023) www.kontron.com // 210
**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.
Disabling server access to the I210 Ethernet controller

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

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

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
Configuring sensors and thermal parameters

Table of contents
- Performing configurations using Redfish
  - Configuring sensor thresholds
  - Configuring minimum fan speed
  - Configuring maximum fan speed
  - Configuring a threshold offset
  - Configuring a start point offset from threshold
  - Configuring the minimum ambient temperature
- Performing configurations using IPMI
  - Configuring thresholds

**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 cannot be populated nor configured.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Identify the URL to use in order to change the thresholds and the sensor name.</td>
</tr>
</tbody>
</table>
| 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

### Configuring minimum fan speed

Version 1.0 (March 2023)
Minimum fan speed should never be under 30%.

### 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.

### 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 sent for nothing near threshold values.

### 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.

### 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 value, fans are stopped so the heater can do its work in a cold environment.

### 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, change the threshold value of the desired sensor.

LocalServer_OSPrompt:~# ipmitool sensor thresh "[SENSOR_ID]" [THRESH_TYPE] [VALUE]

Supported_THRESHOLDS are:
- unr = upper non-recoverable
- ucr = upper critical
- unc = upper non-critical
- lnc = lower non-critical
- lcr = lower critical
- lnr = lower non-recoverable

Version 1.0 (March 2023) www.kontron.com
Operating
Platform power management

Table of contents
- Integrated server power management
  - Integrated server power management using the BMC Web UI
  - Integrated server power management using Redfish
  - Integrated server power management using IPMI over LAN (IOL)
- Rebooting the BMC
  - Rebooting the BMC using the BMC Web UI
  - Rebooting the BMC using Redfish
- Rebooting the switch NOS
  - Rebooting the switch NOS using the NOS CLI
  - Rebooting the switch NOS using the NOS Web UI

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' -d '{"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.
```
```

### 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.
```
```

### Step 2
Execute the power action command from the commands listed.
```
```

### Step 3
Verify the 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:  
```
$ 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.
<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the left-side menu, select <strong>Maintenance</strong> and then <strong>Restart Device</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click on the <strong>Yes</strong> button to begin the restart procedure.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Wait for the switch to be available again.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>Rebooting the switch NOS may take several seconds.</td>
</tr>
</tbody>
</table>

**NOTE:** If the switch NOS is rebooted, some switches may not become available immediately. Please wait for the switch to become available again.
BMC session management

Table of contents
- Viewing BMC sessions
  - Viewing BMC sessions using the BMC Web UI
  - Viewing BMC sessions using Redfish
- Disconnecting BMC sessions
  - Disconnecting BMC sessions using the BMC Web UI
  - Disconnecting a BMC session using Redfish
- Configuring BMC session timeout
  - Configuring BMC session timeout using Redfish
- Redfish token-based authentication
  - Prerequisites
  - Creating a session token

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
```

```
"@odata.id": ["redfish/v1/SessionService/Sessions/", "@odata.type": "+SessionCollection.SessionCollection", "@odata.context": "+SessionCollection", "Members": [ ] }
```

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
```

```
"@odata.id": ["redfish/v1/SessionService/Sessions/Session/", 
"@odata.type": "+Session.v1_1_0.Session", 
"SessionId": "1", 
"Status": "PowerState", 
"UserName": "root", 
"Password": ","]
```

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.
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

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.

Display the current BMC session timeout value.


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.

```bash
```

**Step_2** Extract the token from the response header from the temporary file and delete it.

```bash
```

**Step_3** Verify that the token is valid by accessing a Redfish resource. Add the token as an additional header.

```bash
```
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.

**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.
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.

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.

```
```

**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] [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 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 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.

```
```

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 IDL. To use IDL, add the IDL parameters to the command:

```
```

Version 1.0 (March 2023)  www.kontron.com
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

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 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 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 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
Identify the type of IO module using the following command.
```
$ curl -k -s --request GET --url https://admin:ready@ip172.16.182.31/redfish/v1/Chassis
```
```
```

Step_2
Collect the IO module information using the following command and the URL obtained at the previous step.
```
$ curl -k -s --request GET --url https://admin:ready@ip172.16.182.31/redfish/v1/Chassis/
```
```
```

Collecting product IO module 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:
```
```

Step_1
Use the following command to collect the FRU information.
LocalServer_OSPrompt:$ ipmitool fru print
```
# ipmitool fru print
```
```
IO module type:
Switchboard = ME1310-SW-X
IOBoard = ME1310-I06
```

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

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

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 memory device information using the following command.
```
```

---

Version 1.0 (March 2023)  www.kontron.com  // 234
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.
```

```
LocalSwitchNOS_OSPrompt:~# copy <running-config|startup-config> scp://<SERVER_USERNAME>:<SERVER_PASSWORD>@<SERVER_IP>/<FILE_PATH> save-host-key
```

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

```
```

Version 1.0 (March 2023)  www.kontron.com // 235
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
- General monitoring procedure for unit-based sensors
  - Monitoring using the BMC Web UI
  - Monitoring using Redfish
    - Creating URL extensions
    - Viewing sensor details
  - Monitoring using IPMI
- Discrete sensor monitoring procedure
  - Board Reset
    - Possible values (IPMI only)
    - Monitoring Board Reset using IPMI
    - Monitoring last reset time
  - Heaters
    - Possible values
    - Monitoring heaters using Redfish
    - Monitoring heaters using IPMI
  - Intrusion
    - Event assertion
    - Event deassertion
  - IPMIWatchdog
  - Jumpers Status
    - Monitoring Jumpers Status sensor using Redfish
    - Monitoring Jumpers Status sensor using IPMI
  - TelcoAlarms
    - Monitoring TelcoAlarms using Redfish
    - Monitoring TelcoAlarms using IPMI
    - Event assertion
    - Event deassertion

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.

<table>
<thead>
<tr>
<th>Type</th>
<th>URL extensions</th>
<th>Parser arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan sensors</td>
<td>Chassis / ME1310_Baseboard / Thermal</td>
<td>jq &quot;.Fans&quot;</td>
</tr>
<tr>
<td>Temperature sensors (including PSU sensors)</td>
<td>Chassis / ME1310_Baseboard / Thermal</td>
<td>jq &quot;.Temperatures&quot;</td>
</tr>
<tr>
<td>Voltage sensors (including PSU sensors)</td>
<td>Chassis / ME1310_Baseboard / Power</td>
<td>jq &quot;.Voltages&quot;</td>
</tr>
<tr>
<td>Power sensors (including PSU sensors)</td>
<td>Chassis / ME1310_Baseboard / Sensors</td>
<td>jq</td>
</tr>
<tr>
<td>Other unit-based sensors</td>
<td>Chassis / ME1310_Baseboard / Sensors</td>
<td>jq</td>
</tr>
<tr>
<td>Discrete sensors</td>
<td>Managers/bmc</td>
<td>jq &quot;.Dem.Kontron.Discrete&quot;</td>
</tr>
<tr>
<td>Pass-through IO module sensors</td>
<td>Chassis / IOBoard / Thermal</td>
<td>jq &quot;.Temperatures&quot;</td>
</tr>
<tr>
<td>Ethernet switch IO module sensors</td>
<td>Chassis / Switchboard / Thermal</td>
<td>jq &quot;.Temperatures&quot;</td>
</tr>
</tbody>
</table>

**Viewing sensor details**

Version 1.0 (March 2023)  www.kontron.com // 239
Step_1
归属于传感器类型的URL后添加合适的扩展名。请参阅上述URL扩展名表。
RemoteComputer_OSPrompt:~/
curl -k -s --request GET --url [ROOT_URL]/redfish/v1/[URL_EXTENSION] [PARSER_ARGUMENT]
[PARSER_ARGUMENT]
[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, enter the command.
LocalServer_OSPrompt:~#

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.
<table>
<thead>
<tr>
<th>Event offset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>Unexpected power loss</td>
</tr>
<tr>
<td>0x02</td>
<td>Power cycle or serial port reset</td>
</tr>
<tr>
<td>0x06</td>
<td>Cold reset</td>
</tr>
<tr>
<td>0x07</td>
<td>Power reset from IPMI command</td>
</tr>
</tbody>
</table>

**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**

Version 1.0 (March 2023)
- 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

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Device disabled</td>
</tr>
<tr>
<td>1</td>
<td>Device enabled</td>
</tr>
</tbody>
</table>

**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.

```bash
```

**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 IDL. To use IDL, add the IOL parameters to the command:

```
```

**Step 1**
Display the heaters’ statuses using the following command.

```bash
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

**Intrusion**

The chassis intrusion sensor will register an event if the chassis is opened. This sensor needs manual deassertion.

**Relevant sections:**
- Sensor list
- System event log

**Event assertion**

The chassis intrusion sensor will register an event in the following circumstances:
- When the chassis is opened – the BMC will register a critical chassis intrusion event in the system event log.
- When the chassis intrusion sensor is manually deasserted – the BMC will register a chassis intrusion reset event in the system event log.

**Event deassertion**

This sensor needs manual deassertion. If a chassis intrusion occurs, the sensor’s state needs to be manually reset. Redfish is the only supported way for event deassertion.

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.

---

Version 1.0 (March 2023) 
www.kontron.com
Step_1  Manually change the sensor's value using the following command:

```bash
RemoteComputer_OSPrompt:~# curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/Chassis/ME1310_Baseboard --header 'Content-Type: application/json' --data "{'PhysicalSecurity': {'IntrusionSensor': 'Normal'}}" | jq
```

**NOTE:** As of the current BMC firmware version, the BMC health status will be in a critical state as long as there are critical events in the system event log. Currently, the only supported way of restoring the BMC health status is by clearing the system event log. Refer to [System event log](#) for further instructions. It is recommended to export all system event log entries beforehand.

**IPMIWatchdog**

The IPMIWatchdog sensor will report a critical event in the system event log when it expires because an error prevents the platform from booting correctly.

**Relevant sections:**
- [Sensor list](#)
- [System event log](#)

**Jumpers Status**

Jumpers Status sensor values are reserved and should never differ from the default values shown below. Otherwise, it could render the platform inoperable.

**Relevant section:**
- [Sensor list](#)

**Monitoring Jumpers Status sensor using Redfish**

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.**

```bash
```

**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 IDL. To use IDL, add the IDL 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 Port connector. The BMC will register an event indicating a status change. Refer to [Connector pinouts and electrical characteristics](#) for pinout.

**NOTE:** If no normally-closed contacts are connected to the front panel, the BMC will register a critical event in the system event log each time it reboots because it will assume it detects faulty hardware or a cut wire. Refer to [System event log](#) for a description of what happens in the SEL upon reboot with regards to TelcoAlarms.

There are seven TelcoAlarm sensors present in the platform:

- TelcoAlarm1
- TelcoAlarm2
- TelcoAlarm3
- TelcoAlarm4
- TelcoAlarm5
- TelcoAlarm6
- TelcoAlarm7
### 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.

```
```

Possible values are:

- 0 for a closed contact
- 1 for an open contact

![Redfish output example](redfish_output.png)

---

### 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

![IPMI output example](ipmi_output.png)

---

#### Event assertion

The TelcoAlarm sensors will register an event in the following circumstances:

- When a TelcoAlarm input changes from closed to open – the BMC will register a critical TelcoAlarm event in the system event log.
- When a TelcoAlarm input changes from open to closed – the BMC will register a TelcoAlarm restoration event in the system event log, but note that a restoration event does not deassert a critical TelcoAlarm event.

#### Event deassertion

This event cannot be deasserted.

**NOTE:** As of the current BMC firmware version, the BMC health status will be in a critical state as long as there are critical events in the system event log. Currently, the only supported way of restoring the BMC health status is by clearing the system event log. Refer to [System event log](#) for further instructions. It is recommended to export all system event log entries beforehand.
Sensor list

Table of contents
- **ME1310 sensors**
  - Unit-based sensors
    - Fan sensors
    - Temperature sensors
    - Voltage sensors
    - Power sensors
    - Other unit-based sensors
  - Discrete sensors
    - Power supply sensors
      - DC PSU sensors
      - AC PSU sensors
    - IO module sensors
      - Ethernet switch IO module sensors
      - Pass-through IO module sensors
  - Application-specific sensors
    - Silicom P3iMB sensors

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**

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan 1</td>
<td>FAN 1 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Fan 2</td>
<td>FAN 2 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Fan 3</td>
<td>FAN 3 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Fan 4</td>
<td>FAN 4 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Fan 5</td>
<td>FAN 5 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Fan 6</td>
<td>FAN 6 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Fan 7</td>
<td>FAN 7 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Fan 8</td>
<td>FAN 8 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>

**Temperature sensors**

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp CPU</td>
<td>Internal CPU temperature</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp BMC</td>
<td>Temperature under BMC</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp CPU Area</td>
<td>Temperature under CPU</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp Chassis</td>
<td>Temperature from chassis thermistor Refer to <a href="#">Installing a thermal probe for the PCIe add-in card</a> for thermal probe location.</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp DIMMA1</td>
<td>Temperature of DIMM 1 on channel A</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp DIMMA2</td>
<td>Temperature of DIMM 2 on channel A</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp DIMMB1</td>
<td>Temperature of DIMM 1 on channel B</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp</td>
<td>Temperature of DIMM 2 on channel B</td>
<td>Temperature</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Sensor name</td>
<td>Description</td>
<td>Sensor type code</td>
<td>Event/Reading type code</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>DIMMB2</td>
<td>Temperature of DIMM 1 on channel C</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DIMMC1</td>
<td>Temperature of DIMM 2 on channel C</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DIMMC2</td>
<td>Temperature of DIMM 1 on channel D</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DIMMD1</td>
<td>Temperature of DIMM 2 on channel D</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DIMMD2</td>
<td>Temperature under FPGA</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp Inlet</td>
<td>Temperature of fresh air inlet</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp M2 Area</td>
<td>Temperature near M.2 J8 and J9</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp PCIe 1</td>
<td>Temperature from PCIe slot 1 thermistor</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp PCIe 1 mbox</td>
<td>Temperature from PCIe slot 1 reported via mailbox</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp PCIe 2</td>
<td>Temperature from PCIe slot 2 thermistor</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp PCIe 2 mbox</td>
<td>Temperature from PCIe slot 2 reported via mailbox</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp PSU Outlet</td>
<td>Temperature of system PSU outlet</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp VCCIN</td>
<td>Temperature near VCCIN switcher</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp VDDQ_AB</td>
<td>Temperature near VDDQ_AB switcher</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp VDDQ_CD</td>
<td>Temperature near VDDQ_CD switcher</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp V_3V3_SUS</td>
<td>Temperature near V_3V3_SUS switcher</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>

Voltage sensors

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>VBAT</td>
<td>RTC battery voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_3V3_M2</td>
<td>V_3V3_M2 voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_3V3_PCH_AUX</td>
<td>V_3V3_PCH_AUX voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_3V3_RGM_BMC</td>
<td>V_3V3_RGM_BMC voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_3V3_SLOT</td>
<td>V_3V3_SLOT voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_12V_SLOT1</td>
<td>V_12V_SLOT1 voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_12V_SLOT2</td>
<td>V_12V_SLOT2 voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_12V_SUS</td>
<td>V_12V_SUS voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_VTT_AB</td>
<td>V_VTT_AB voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>V_VTT_CD</td>
<td>V_VTT_CD voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>

Power sensors

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>P_12V SLOT1</td>
<td>V_12V_SLOT1 power consumption</td>
<td>Power Supply (0x08)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>P_12V SLOT2</td>
<td>V_12V_SLOT2 power consumption</td>
<td>Power Supply (0x08)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>

Other unit-based sensors
Version 1.0 (March 2023) www.kontron.com // 246
### Other unit-based sensors

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humidity</td>
<td>Relative humidity at air inlet</td>
<td>Other Units-based sensor (0x0B)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>

### Discrete sensors

For information about discrete sensors, refer to [Discrete sensor monitoring procedure](#).

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heater CPU</td>
<td>Heater status indicator for CPU</td>
<td>Chassis (0x18)</td>
<td>0x9 ('digital' Discrete - Device Disabled/Device Enabled)</td>
</tr>
<tr>
<td>Heater PCIe1</td>
<td>Heater status indicator for PCIe1</td>
<td>Chassis (0x18)</td>
<td>0x9 ('digital' Discrete - Device Disabled/Device Enabled)</td>
</tr>
<tr>
<td>Heater PCIe2</td>
<td>Heater status indicator for PCIe2</td>
<td>Chassis (0x18)</td>
<td>0x9 ('digital' Discrete - Device Disabled/Device Enabled)</td>
</tr>
<tr>
<td>Intrusion</td>
<td>Alarm status from front panel connector</td>
<td>Platform Alert (0x24)</td>
<td>0x3 ('digital' Discrete - Assert/Deassert)</td>
</tr>
<tr>
<td>TelcoAlarm1</td>
<td>Status from front panel alarm connector</td>
<td>Platform Alert (0x24)</td>
<td>0x3 ('digital' Discrete - Assert/Deassert)</td>
</tr>
<tr>
<td>TelcoAlarm2</td>
<td>Status from front panel alarm connector</td>
<td>Platform Alert (0x24)</td>
<td>0x3 ('digital' Discrete - Assert/Deassert)</td>
</tr>
<tr>
<td>TelcoAlarm3</td>
<td>Status from front panel alarm connector</td>
<td>Platform Alert (0x24)</td>
<td>0x3 ('digital' Discrete - Assert/Deassert)</td>
</tr>
<tr>
<td>TelcoAlarm4</td>
<td>Status from front panel alarm connector</td>
<td>Platform Alert (0x24)</td>
<td>0x3 ('digital' Discrete - Assert/Deassert)</td>
</tr>
<tr>
<td>TelcoAlarm5</td>
<td>Status from front panel alarm connector</td>
<td>Platform Alert (0x24)</td>
<td>0x3 ('digital' Discrete - Assert/Deassert)</td>
</tr>
<tr>
<td>TelcoAlarm6</td>
<td>Status from front panel alarm connector</td>
<td>Platform Alert (0x24)</td>
<td>0x3 ('digital' Discrete - Assert/Deassert)</td>
</tr>
<tr>
<td>TelcoAlarm7</td>
<td>Status from front panel alarm connector</td>
<td>Platform Alert (0x24)</td>
<td>0x3 ('digital' Discrete - Assert/Deassert)</td>
</tr>
<tr>
<td>IPMIWatchdog</td>
<td>IPMI Watchdog action reporting</td>
<td>Watchdog 2 (0x23)</td>
<td>0x6f (Sensor Specific)</td>
</tr>
<tr>
<td>Board Reset</td>
<td>Reports the last reset source</td>
<td>Board Reset (Kontron OEM) (0xC4)</td>
<td>0x6f (Sensor Specific)</td>
</tr>
<tr>
<td>Jumpers Status</td>
<td>Reserved – event-based sensor</td>
<td>Jumpers Status - Kontron OEM (0x03)</td>
<td>0x6f (Sensor Specific)</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC PSU Pout</td>
<td>Output power from PSU</td>
<td>Power Supply (0x0B)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU Vout</td>
<td>DC PSU 48V to 12V regulator output voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU Iout</td>
<td>DC PSU 48V to 12V regulator output current</td>
<td>Current (0x03)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU Regulator</td>
<td>Temperature in the DC PSU 48V to 12V regulator</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU HoldUp</td>
<td>Temperature in the DC PSU HoldUp generation regulator</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU Inlet</td>
<td>Temperature in the DC PSU feed ORing circuit</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU HVout</td>
<td>DC PSU hold up voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU Vin</td>
<td>DC PSU QBrick input voltage</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU Feed A</td>
<td>DC PSU FPGA Feed A reading</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>DC PSU Feed B</td>
<td>DC PSU FPGA Feed A reading</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>
**AC PSU sensors**

NOTE: The AC PSU sensors are only present when an AC PSU is connected.

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC PSU Vout</td>
<td>Output voltage from PSU</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>AC PSU Pout</td>
<td>Output power from PSU</td>
<td>Power Supply (0x08)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>AC PSU Vin</td>
<td>Input voltage from PSU</td>
<td>Voltage (0x02)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>AC PSU Pin</td>
<td>Input power from PSU</td>
<td>Power Supply (0x08)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>AC PSU Temp1</td>
<td>Temperature from PSU</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp SWB Cln</td>
<td>Temperature under ZL30772 DPLL on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB Inlet</td>
<td>Temperature at air inlet on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB OCXO</td>
<td>Temperature under OCXO on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP1</td>
<td>Temperature from SFP1 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP2</td>
<td>Temperature from SFP2 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP3</td>
<td>Temperature from SFP3 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP4</td>
<td>Temperature from SFP4 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP5</td>
<td>Temperature from SFP5 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP6</td>
<td>Temperature from SFP6 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP7</td>
<td>Temperature from SFP7 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP8</td>
<td>Temperature from SFP8 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP9</td>
<td>Temperature from SFP9 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP10</td>
<td>Temperature from SFP10 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP11</td>
<td>Temperature from SFP11 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB SFP12</td>
<td>Temperature from SFP12 module on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>Temp SWB Switch</td>
<td>Temperature from switch die on Ethernet switch IO module</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>

**Pass-through IO module sensors**

NOTE: The pass-through IO module sensors are only present if the platform is equipped with a pass-through IO 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.

<table>
<thead>
<tr>
<th>Sensor name [SENSOR_ID]</th>
<th>Description</th>
<th>Sensor type code</th>
<th>Event/Reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>T P3iMB Local S&lt;X&gt;</td>
<td>Local temperature for Silicom P3iMB PCIe add-in card Where &lt;X&gt; is the PCIe slot ID.</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>T ACC100 TSDE S&lt;X&gt;</td>
<td>Intel ACC100 FEC accelerator TSDE East temperature for Silicom P3iMB PCIe add-in card Where &lt;X&gt; is the PCIe slot ID.</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>T ACC100 TSDW S&lt;X&gt;</td>
<td>Intel ACC100 FEC accelerator TSDW West temperature for Silicom P3iMB PCIe add-in card Where &lt;X&gt; is the PCIe slot ID.</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
</tbody>
</table>
Maintenance
System event log

Table of contents

- BMC system event logs
  - Relationship between BMC system event logs
  - TelcoAlarms registered in the SEL upon BMC reboot
  - Accessing the BMC SEL using the BMC Web UI
    - Accessing the BMC system event log
    - Clearing the BMC system event log
    - Exporting the BMC system event log
  - Accessing the BMC SEL using Redfish
    - Accessing the BMC system event log
    - Clearing the BMC system event log
    - Redfish supported event types
  - Accessing the BMC SEL using IPMI
    - Accessing the BMC system event log
    - Clearing the BMC system event log
    - Exporting the BMC system event log
- NOS system event log
  - Accessing the NOS SEL using the NOS Web UI
    - Accessing the NOS system event log
    - Clearing the NOS system event log
  - Accessing the NOS SEL using the NOS CLI
    - Accessing the NOS system event log
    - Clearing the NOS system event log

BMC system event logs

The BMC system event log 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.

TelcoAlarms registered in the SEL upon BMC reboot

TelcoAlarms are used to detect statuses of the inputs of the front panel alarm connector. If nothing is connected to the Alarm Port, TelcoAlarm events will be registered in the SEL if a BMC reboot occurs. This happens because in order to detect faulty wiring (a cut cable, etc.) the system considers an open loop as an event—and an empty Alarm Port creates an open loop.

If the Alarm Port is not used, a solution would be to install a loop back RJ45 connector assembly into the Alarm Port.

The TelcoAlarms generated will set the BMC health status in a critical state. Currently, the only supported way of restoring the BMC health status is by clearing the system event log. Kontron recommends exporting the SEL before clearing it.

Relevant section:

Platform components

Accessing the 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 Version 1.0 (March 2023)

www.kontron.com // 251
### 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 access 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:admin@172.16.182.11/redfish/v1/Systems/system/LogServices/EventLog/Entries | jq
```

#### Step 2
Verify that the system event log was properly cleared.


```
$ curl -k -s --request POST --url https://admin:admin@172.16.182.11/redfish/v1/Systems/system/LogServices/EventLog/Actions/LogService.ClearLog | jq
```

#### 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.
<table>
<thead>
<tr>
<th>Event type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InventoryAdded</td>
<td>Indicates that an inventory item with the specified model, type, and serial number was installed.</td>
</tr>
<tr>
<td>InventoryRemoved</td>
<td>Indicates that an inventory item with the specified model, type, and serial number was removed.</td>
</tr>
<tr>
<td>BoardReset</td>
<td>Indicates that the payload was reset.</td>
</tr>
<tr>
<td>DCPowerOn</td>
<td>Indicates that the system DC power is on.</td>
</tr>
<tr>
<td>DCPowerOff</td>
<td>Indicates that the system DC power is off.</td>
</tr>
<tr>
<td>SensorThresholdCriticalLowGoingLow</td>
<td>Indicates that a threshold sensor has crossed a critical low threshold going low.</td>
</tr>
<tr>
<td>SensorThresholdCriticalLowGoingHigh</td>
<td>Indicates that a threshold sensor has crossed a critical low threshold going high.</td>
</tr>
<tr>
<td>SensorThresholdCriticalHighGoingLow</td>
<td>Indicates that a threshold sensor has crossed a critical high threshold going low.</td>
</tr>
<tr>
<td>SensorThresholdCriticalHighGoingHigh</td>
<td>Indicates that a threshold sensor has crossed a critical high threshold going high.</td>
</tr>
<tr>
<td>SensorThresholdWarningLowGoingLow</td>
<td>Indicates that a threshold sensor has crossed a warning low threshold going low.</td>
</tr>
<tr>
<td>SensorThresholdWarningLowGoingHigh</td>
<td>Indicates that a threshold sensor has crossed a warning low threshold going high.</td>
</tr>
<tr>
<td>SensorThresholdWarningHighGoingLow</td>
<td>Indicates that a threshold sensor has crossed a warning high threshold going low.</td>
</tr>
<tr>
<td>SensorThresholdWarningHighGoingHigh</td>
<td>Indicates that a threshold sensor has crossed a warning high threshold going high.</td>
</tr>
<tr>
<td>FanRedundancyLost</td>
<td>Indicates that system fan redundancy has been lost.</td>
</tr>
<tr>
<td>FanRedundancyRegained</td>
<td>Indicates that system fan redundancy has been regained.</td>
</tr>
<tr>
<td>FanSpeedDeviated</td>
<td>Indicates that fan speed has deviated from target, could indicate a faulty fan.</td>
</tr>
<tr>
<td>FanSpeedRestored</td>
<td>Indicates that fan speed is now back to normal.</td>
</tr>
<tr>
<td>IPMIWatchdog</td>
<td>Indicates that IPMI watchdog timed out.</td>
</tr>
</tbody>
</table>

### 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

Version 1.0 (March 2023)

www.kontron.com
Step_1

Use the following command to save the system event log into a file.

```
LocalServer_OSPrompt:~# ipmitool sel save [FILE_NAME]
```

**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 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**

Version 1.0 (March 2023)
| Step 1 | Display the switch NOS event log.  
LocalSwitchNOS_OSPrompt:~# `show logging` |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image1" alt="Event Log Display" /></td>
</tr>
<tr>
<td></td>
<td>Clearing the NOS system event log</td>
</tr>
<tr>
<td></td>
<td><img src="image2" alt="Clearing Log" /></td>
</tr>
<tr>
<td>Step 2</td>
<td>The NOS system event log should be empty.</td>
</tr>
<tr>
<td></td>
<td>LocalSwitchNOS_OSPrompt:~# <code>show logging</code></td>
</tr>
<tr>
<td></td>
<td><img src="image3" alt="Empty Log" /></td>
</tr>
</tbody>
</table>
POST code logs

Table of contents
- Accessing the POST code logs using the BMC Web UI
- Accessing the POST code logs using Redfish

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_DSPrompt:~# curl -k -s --request GET --url [ROOT_URL]/redfish/v1/Systems/system/LogServices/PostCodes/Entries | jq
Interpreting sensor data

Table of contents
- Interpretation procedure
- Interpretation information
  - Sensor type
  - Sensor event and reading type
    - Threshold-based event and reading type

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.

<table>
<thead>
<tr>
<th>Sensor Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0 (March 2023)</td>
<td><a href="http://www.kontron.com">www.kontron.com</a></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Event/reading type</th>
<th>7-bit event type code</th>
<th>Description</th>
<th>Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold based</td>
<td>01h</td>
<td>Unit-based sensors, meaning it has a numerical reading and event triggers</td>
<td>Offsets are standard and defined in the Threshold-based event and reading type table</td>
</tr>
</tbody>
</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.

<table>
<thead>
<tr>
<th>Event offset</th>
<th>Event trigger</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>00h</td>
<td>Lower noncritical – going low</td>
<td>nc</td>
</tr>
<tr>
<td>01h</td>
<td>Lower noncritical – going high</td>
<td></td>
</tr>
<tr>
<td>02h</td>
<td>Lower critical – going low</td>
<td>cr</td>
</tr>
<tr>
<td>03h</td>
<td>Lower critical – going high</td>
<td></td>
</tr>
<tr>
<td>04h</td>
<td>Lower non-recoverable – going low</td>
<td>nr</td>
</tr>
<tr>
<td>05h</td>
<td>Lower non-recoverable – going high</td>
<td></td>
</tr>
<tr>
<td>06h</td>
<td>Upper noncritical – going low</td>
<td>nc</td>
</tr>
<tr>
<td>07h</td>
<td>Upper noncritical – going high</td>
<td></td>
</tr>
<tr>
<td>08h</td>
<td>Upper critical – going low</td>
<td>cr</td>
</tr>
<tr>
<td>09h</td>
<td>Upper critical – going high</td>
<td></td>
</tr>
<tr>
<td>0Ah</td>
<td>Upper non-recoverable – going low</td>
<td>nr</td>
</tr>
<tr>
<td>0Bh</td>
<td>Upper non-recoverable – going high</td>
<td></td>
</tr>
</tbody>
</table>
Component replacement

Refer to Components installation and assembly for component replacement procedures.
Backup and restore

Table of contents
- UEFI/BIOS
  - Backing up the UEFI/BIOS
  - Restoring the UEFI/BIOS
  - Getting information on the latest UEFI/BIOS backup
  - Description of creation and restoration steps
- Switch NOS configuration
  - Backing up and restoring the switch NOS configuration using SCP
  - Backing up and restoring the switch NOS configuration using the switch NOS Web UI

On an ME1310 platform, UEFI/BIOS and switch NOS configurations can be backed up and restored.

UEFI/BIOS

This section describes how to create a UEFI/BIOS backup that includes the current UEFI/BIOS 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
```
The completion code:
- 0x00: Recovery process started successfully
- 0x05: 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
```
The completion code:
- 0x00: Recovery process started successfully
- 0x05: 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

<table>
<thead>
<tr>
<th>Step description</th>
<th>Step value (BYTE1)</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>No step</td>
<td>0x00</td>
<td>Nothing is currently going on, no failure to report.</td>
</tr>
<tr>
<td>Get UEFI/BIOS version</td>
<td>0x01</td>
<td>Retrieve UEFI/BIOS version over DBUS.</td>
</tr>
<tr>
<td>Server Power Off</td>
<td>0x02</td>
<td>Set server to Power Off state.</td>
</tr>
<tr>
<td>Force Intel ME Recovery mode</td>
<td>0x03</td>
<td>Force Intel ME to recovery mode.</td>
</tr>
<tr>
<td>MTD partition detect</td>
<td>0x04</td>
<td>Check flash device and partition are detected.</td>
</tr>
<tr>
<td>MTD Flash erase</td>
<td>0x05</td>
<td>Target flash being erased. Target depends on whether action is CREATE or RESTORE.</td>
</tr>
<tr>
<td>MTD Flash write</td>
<td>0x06</td>
<td>Target flash being written. Target depends on whether action is CREATE or RESTORE.</td>
</tr>
<tr>
<td>MTD Flash verify</td>
<td>0x07</td>
<td>Target flash being verified. Target depends on whether action is CREATE or RESTORE.</td>
</tr>
<tr>
<td>Reset Intel ME to Normal mode</td>
<td>0x08</td>
<td>Reset Intel ME to return to normal mode.</td>
</tr>
<tr>
<td>Server Power On</td>
<td>0x09</td>
<td>Set server to Power On state.</td>
</tr>
</tbody>
</table>

Switch NOS configuration

This section describes how to backup and restore the switch NOS configuration. These operations can be achieved:
- Using SCP
- Using the switch NOS Web UI

Backing up and restoring the switch NOS configuration using SCP

Prerequisites

1. A server configured for the desired protocol is available and accessible from the switch NOS.
2. If restoring a configuration, the corresponding configuration file is present on the server.

The URL following the server IP address is a path relative to the user home folder provided (~/). To specify an absolute path, use a double slash after the IP address (e.g. scp://<SERVER_USERNAME>:<SERVER_PASSWORD>@<SERVER_IP>/<path/to/configfile>).

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

Backing up the switch NOS configuration

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.

LocalswitchNOS_OSPrompt: ~# copy <running-config> startup-config scp://<SERVER_USERNAME>:<SERVER_PASSWORD>@<SERVER_IP>/<FILE_PATH> save-host-key

Restoring the switch NOS configuration

Version 1.0 (March 2023)  www.kontron.com // 262
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Access the switch network operating system using SSH or a serial connection.</td>
</tr>
</tbody>
</table>
| Step 2 | Copy the configuration file from the remote server as one of the following:  
- **running-config**: configuration currently active (volatile until saved as startup-config).  
- **startup-config**: saved configuration applied at switch boot.  
LocalSwitchNOS_0SPrompt:~# copy scp://<SERVER_USERNAME>:<SERVER_PASSWORD>@<SERVER_IP>/<FILE_PATH> <running-config|startup-config> save-host-key |
| Step 3 | If the configuration was written to the startup-config, the switch NOS must be rebooted for the changes to take effect.  
LocalSwitchNOS_0SPrompt:~# reload cold |

### Backing up and restoring the switch NOS configuration using the switch NOS Web UI

Access the switch NOS Web UI. Refer to [Accessing the switch NOS](#) for access instructions.

#### Backing up the switch NOS configuration

| 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
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
  - Prerequisites
  - Procedure
- Upgrading FPGA firmware
  - Prerequisites
  - Procedure
- Upgrading UEFI/BIOS firmware
  - Prerequisites
  - Procedure
- Upgrading switch firmware
  - Prerequisites
  - Procedure

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The .tar file provided by Kontron was downloaded on the remote computer.</td>
</tr>
<tr>
<td>2</td>
<td>Access to the BMC Redfish interface is required.</td>
</tr>
</tbody>
</table>

Relevant section:
- Accessing a BMC using Redfish

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>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</td>
</tr>
<tr>
<td>Step_2</td>
<td>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</td>
</tr>
</tbody>
</table>
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.
```
$ curl -k -s --request GET --url [ROOT_URL]/redfish/v1/UpdateService/FirmwareInventory/ [FIRMWARE_ID] | jq ".Description,.Version"
```

Step 4
Set the apply time to Immediate.
```
$ curl -k -s --request PATCH --url [ROOT_URL] /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.
```
```

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.
```
```

Step 7
Once the BMC becomes available again, verify that the firmware version has changed.
```
$ curl -k -s --request GET --url [ROOT_URL] /redfish/v1/Managers/bmc | jq .FirmwareVersion
```

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.

```bash
RemoteComputer_OSPrompt:
$ curl -k -s -X GET --url [ROOT_URL]/redfish/v1/Systems/system | jq .FpgaVersion
```

Step_2
Collect all the IDs of the firmware present on the platform.

```bash
RemoteComputer_OSPrompt:
$ curl -k -s -X GET --url [ROOT_URL]/redfish/v1/UpdateService/FirmwareInventory | jq .Members
```

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.

```bash
RemoteComputer_OSPrompt:
$ curl -k -s -X GET --url [ROOT_URL]/redfish/v1/UpdateService/FirmwareInventory/ [FIRMWARE_ID] | jq ".Description,.Version"
```

Step_4
Set the apply time to Immediate.

```bash
RemoteComputer_OSPrompt:
$ curl -k -s -X PATCH --url [ROOT_URL]/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.

```bash
RemoteComputer_OSPrompt:
$ curl -k -s -X POST --url [ROOT_URL]/redfish/v1/UpdateService --header 'Content-Type: application/octet-stream' --upload-file "[FILE_PATH]" | jq
```

Step_6
Once the BMC becomes available again, verify that the firmware version has changed.

```bash
RemoteComputer_OSPrompt:
$ curl -k -s -X GET --url [ROOT_URL]/redfish/v1/Systems/system | jq .FpgaVersion
```

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 a virtual media and the built-in UEFI shell

Upgrading UEFI/BIOS firmware using a virtual media and the built-in UEFI shell

Prerequisites

1 A virtual media .bin file has been provided by Kontron.
2 Access to the BMC Web UI is required.
3 Secure Boot must be disabled.

Relevant sections:
Accessing the UEFI or BIOS
Accessing a BMC using the Web UI

Mounting the UEFI/BIOS upgrade virtual media
Step_1  From the left-side menu of the BMC Web UI, select Operations and then Virtual media.

Step_2  Click on Add file to browse for the .bin file provided by Kontron.

Step_3  Click on Start.

Upgrading the UEFI/BIOS
Step_1  Access the UEFI/BIOS setup menu.

Step_2  From the UEFI/BIOS setup menu, navigate to the Save & Exit menu.

Step_3  Select the UEFI: Built-in EFI Shell option from the Boot Override menu.

Step_4  The built-in EFI Shell should launch. Do not press any key. Wait for the message “BIOS UPDATE STARTING”.

Step_5  When prompted, press any key other than ‘q’ to continue. The UEFI/BIOS upgrade should start.

Step_6  At the end of the upgrade process, press the Enter key to end the UEFI/BIOS upgrade.

Step_7  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 switch firmware

Switch firmware can be upgraded using:

- SCP
- The switch NOS Web UI

NOTE: The switch startup configuration will not be affected by a switch firmware upgrade.

Upgrading switch firmware using SCP

Prerequisites

1. A server configured for the desired protocol is available and accessible from the switch NOS.
2. The .itb upgrade file provided by Kontron was downloaded on the server.

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]).
### Upgrading switch firmware using the switch NOS Web UI

#### Prerequisites

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access to the switch NOS Web UI is required.</td>
</tr>
<tr>
<td>2</td>
<td>The <code>.itb</code> upgrade file provided by Kontron was downloaded on the remote computer.</td>
</tr>
</tbody>
</table>

#### Relevant section:

Accessing the switch NOS using the switch NOS Web UI

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From the left-side menu of the switch NOS Web UI, select <strong>Maintenance</strong>, <strong>Software</strong> and then <strong>Upload</strong>.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Click the <strong>Select File</strong> button and then choose the desired <code>.itb</code> file.</td>
</tr>
<tr>
<td>Step_3</td>
<td>After selecting the file for the upgrade, click on <strong>Start Upgrade</strong>.</td>
</tr>
<tr>
<td>Step_4</td>
<td>Wait for the upload and upgrade process to complete.</td>
</tr>
<tr>
<td>Step_5</td>
<td>Once the upgrade is done, from the left-side menu, select <strong>Monitor</strong>, <strong>System</strong> and then <strong>Information</strong>. Confirm that the <strong>Software Version</strong> corresponds to that of the <code>.itb</code> file.</td>
</tr>
</tbody>
</table>
Platform cooling and thermal management

Table of contents
- Behavior upon startup at temperatures below 0 degrees Celsius
- Behavior at temperatures below or above 10 degrees Celsius
- Cooling management
  - Cooling management characteristics
  - Fan fault detection method
  - Default temperature thresholds

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 needs to be heated before startup. Heating elements are built-in for the CPU and, optionally, for the PCIe add-in cards.
- When the platform is started at temperatures below 0°C, an internal heating element preheats the components sensitive to cold prior to the board power on.
- Once the temperature of these components exceeds 0°C, the server is powered on.

This behavior is communicated through platform LEDs. For more information, refer to General platform LEDs.

Behavior at temperatures below or above 10 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 8% of their maximum capacity.
- If, at any ambient temperature, it is detected that a sensor reaches its Upper non-critical threshold, fan cooling will engage to ensure that no component is overheating.

Cooling management

The cooling management of the platform is handled by an integrated BMC. The BMC uses information collected from on-board temperature sensors to adjust the speed of the fans and regulate the temperature of the platform. For each sensor, the temperature reading is compared against corresponding configured thresholds to determine the required fan speed. The resulting duty cycle is based on cooling parameters, such as minimum and maximum fan speed, and gets linearly increased when a temperature reading gets between the Upper non-critical and Upper critical thresholds for that sensor. The fan control behavior can be fine-tuned by configuring these thresholds to match the target environment.

In addition to the sensors read by the BMC, other sensors can be read by a customer application, if available, running under the server’s OS and then reported to the BMC. As such, PCIe add-in card temperatures, as well as M.2 and SFP temperatures, can be reported to the BMC by the customer application and
Cooling management characteristics

- Minimum fan speeds are set to 8%.
- Minimum ambient temperature is set to 10°C. Above this temperature, fans will be running. Below this temperature, fans will be stopped but ready to start if a component requires cooling.
- Fans are started before reaching their threshold value using a threshold offset parameter.
- Fan speed deviation is monitored for failure.
- A watchdog timer sets fans to 100% if the BMC does not issue control commands. This will normally occur while the BMC reboots, for example, during a firmware upgrade.
- A BMC firmware upgrade failsafe sets fan speed to 100% during a BMC firmware upgrade or reboot.
- A small negative slew rate applies on fan speed to ensure a slow decrease in fan speed and prevent fan oscillation.
- Fast response to temperature rise.
- Fan redundancy.

Fan fault detection method

To detect faulty fans, the speed of each fan is continuously monitored and compared to the target value sent by the fan controller. If the fan speed is out of range by ±15% for 30 seconds, the fan is marked as faulty and a Redfish event is sent. The fan can later be restored if the speed comes back within the deviation range for a steady period of 5 seconds.

All the fans are redundant. This means that when a fan is faulty, all the other healthy fans will be set to maximum speed.

To access the SEL using Redfish to see the events, refer to System event log.

Default temperature thresholds

To see temperature thresholds, refer to the instructions provided in Monitoring sensors and Configuring sensors and thermal parameters.
Troubleshooting
Collecting diagnostics

Table of contents
- Collecting the system inventory
- Collecting the event logs
- Collecting system information using a QR code

The following information could be required when contacting the support team to make the proper board health diagnostics. However, if the platform is inoperable, 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.

Collecting system information using a QR code

Relevant section: MAC addresses

<table>
<thead>
<tr>
<th>Step 1</th>
<th>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).</th>
</tr>
</thead>
<tbody>
<tr>
<td>S/N: 9017020001</td>
<td>Platform serial number</td>
</tr>
<tr>
<td>P/N: 1065-2823</td>
<td>Platform part number</td>
</tr>
<tr>
<td>BATCH: 0A00000001</td>
<td>Platform production lot number</td>
</tr>
<tr>
<td>MAC: 00A0A5D6402A</td>
<td>First MAC address attributed to the BMC/server. Value to be used to replace MAC_BASE.</td>
</tr>
<tr>
<td>00A0A5E1B934</td>
<td>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.</td>
</tr>
<tr>
<td>S/N: 9017020001</td>
<td>Platform serial number</td>
</tr>
<tr>
<td>P/N: 1065-2823</td>
<td>Platform part number</td>
</tr>
<tr>
<td>BATCH: 0A00000001</td>
<td>Platform production lot number</td>
</tr>
<tr>
<td>MAC: 00A0A5D6402A</td>
<td>First MAC address attributed to the BMC/server. Value to be used to replace MAC_BASE.</td>
</tr>
<tr>
<td>00A0A5E1B934</td>
<td>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.</td>
</tr>
</tbody>
</table>
Factory default

Table of contents
  * Restoring default UEFI/BIOS settings
  * Restoring default switch NOS settings
    * Restoring default switch NOS settings using the CLI
    * Restoring default switch NOS settings using the Web UI
  * Restoring a BMC password

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 networking configuration changes. Refer to Description of system access methods to select an appropriate path to access the platform components.

Restoring default switch NOS settings using the CLI

Refer to Accessing the switch NOS for access instructions.

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

Step 1 Restore the default configuration.
LocalSwitchNOS_OSPrompt:~# reload defaults

Step 2 To make the revert to default values permanent, use the following command.
LocalSwitchNOS_OSPrompt:~# copy running-config startup-config

Restoring default switch NOS settings using the Web UI

Refer to Accessing the switch NOS for access instructions.

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

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

Step 1 From the left-side menu, select Maintenance, Configuration and then Activate.

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.

Version 1.0 (March 2023) www.kontron.com // 277
Restoring a BMC password

A BMC administrator password can be restored using the [Accessing a BMC using IPMI (KCS)] method.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Identify the ID of the user with the password to restore.</td>
<td><code>LocalServer_OSPROMPT:~# ipmitool user list [CHANNEL]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="User List" /></td>
</tr>
<tr>
<td>Step 2</td>
<td>Reset the password.</td>
<td><code>LocalServer_OSPROMPT:~# ipmitool user set password [USER_ID] [NEW_PASSWORD]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Password Reset" /></td>
</tr>
</tbody>
</table>
Support information

To ensure 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
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.

![PuTTY Image]

**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                       |
```

**Picocom**

A **BREAK** signal can be sent from the picocom Linux utility's help.

```
*** Picocom commands (all prefixed by [C-a])
...
*** [C-i] : 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify enabled sleep states.</td>
</tr>
<tr>
<td></td>
<td>LocalServer_OSPrompt:~# cat /sys/power/state</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disable sleep states using systemd.</td>
</tr>
<tr>
<td></td>
<td>LocalServer_OSPrompt:~# sudo systemctl mask sleep.target suspend.target hibernate.target hybrid-sleep.target</td>
</tr>
</tbody>
</table>

Disabling sleep states

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disable sleep states using systemd.</td>
</tr>
<tr>
<td></td>
<td>LocalServer_OSPrompt:~# sudo systemctl mask sleep.target suspend.target hibernate.target hybrid-sleep.target</td>
</tr>
</tbody>
</table>

Created symlink from /etc/systemd/system/sleep.target to /dev/null.
Created symlink from /etc/systemd/system/suspend.target to /dev/null.
Created symlink from /etc/systemd/system/hibernate.target to /dev/null.
Created symlink from /etc/systemd/system/hybrid-sleep.target to /dev/null.
Generating custom secure boot keys

To provision custom secure boot keys, keys may have to be generated. This article provides an example using CentOS 7.

Prerequisites

|   | Packages efitools and sbsigntools must be available. These packages are not official CentOS packages. |

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |
| 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
  - Updating secure boot keys from the UEFI setup utility
  - Prerequisites
  - Procedure

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

Secure Boot is a UEFI-defined feature used to authenticate a UEFI executable, such as an OS loader, using digital signing mechanisms based on the Public Key Infrastructure process, reducing the risks of pre-boot malware attacks. The feature uses a database of authorized signatures to confirm the UEFI executable integrity prior to execution.

Boards will typically have a pre-loaded set of Platform Key (PK), Key Exchange Keys (KEK), authorized signature database (db) and blacklisted / revoked signature database (dbx) as defined by the OEM, as well as some industry-standard certificates issued by Microsoft that allow booting Windows or well-known Linux distributions such as Ubuntu. It may be desirable for an end customer to update these keys with their own set for security reasons.

This document assumes the reader has some knowledge about the Secure Boot process, and that the required set of keys and certificates has been properly generated. The following link provides guidelines on creating and managing such keys and certificates:
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-secure-boot-key-creation-and-management-guidance

Updating secure boot keys from the UEFI setup utility

Prerequisites

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

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.
Reference guides
Supported Redfish commands

Table of contents
- Systems URLs
- Managers URLs
- Registries URLs
- Session Service URLs
- Task Service URLs
- Telemetry Service URLs
- Chassis URLs
- Account Service URLs
- Certificate Service URLs
- Update Service URLs
- Event Service URLs
- Miscellaneous URLs

The information is presented in the following format:
- Description  |  URL  |  Type

Schema definition
Schema definition for a specific type can be retrieved 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/Managers/[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
  - Watchdog timer commands
  - BMC device and messaging commands
  - IPMI 2.0 specific commands
- **Chassis commands**
  - Chassis device commands
- **Bridge commands**
  - Bridge management commands
  - Bridge discovery commands
  - Bridging commands
  - Bridge event commands
- **Sensor event commands**
- **Storage commands**
  - FRU information commands
  - SDR repository commands
  - SEL device commands
- **Transport commands**
  - LAN device commands
  - Serial over LAN commands
- **Kontron OEM commands**

### Application commands

#### IPM device commands

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

*Commands are not rejected and can cause unpredictable behavior.*

### Watchdog timer commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x06</td>
<td>0x22</td>
<td>Reset Watchdog Timer</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x24</td>
<td>Set Watchdog Timer</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x25</td>
<td>Get Watchdog Timer</td>
<td>Supported</td>
</tr>
</tbody>
</table>
**BMC device and messaging commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x06</td>
<td>0x2E</td>
<td>Set BMC Global Enables</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x2F</td>
<td>Get BMC Global Enables</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x30</td>
<td>Clear Message Flags</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x31</td>
<td>Get Message Flags</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x32</td>
<td>Enable Message Channel Receive</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x33</td>
<td>Get Message</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x34</td>
<td>Send Message</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x35</td>
<td>Read Event Message Buffer</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x36</td>
<td>Get BT Interface Capabilities</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x37</td>
<td>Get System GUID</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x38</td>
<td>Get Channel Authentication Capabilities</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x39</td>
<td>Get Session Challenge</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3A</td>
<td>Activate Session</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3B</td>
<td>Set Session Privilege Level</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3C</td>
<td>Close Session</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3D</td>
<td>Get Session Info</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3F</td>
<td>Get AuthCode</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x40</td>
<td>Set Channel Access</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x41</td>
<td>Get Channel Access</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x42</td>
<td>Get Channel Info Command</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x43</td>
<td>Set User Access Command</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x44</td>
<td>Get User Access Command</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x45</td>
<td>Set User Name</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x46</td>
<td>Get User Name Command</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x47</td>
<td>Set User Password Command</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x52</td>
<td>Master Write-Read</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x58</td>
<td>Set System Info Parameters</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x59</td>
<td>Get System Info Parameters</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**IPMI 2.0 specific commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x06</td>
<td>0x48</td>
<td>Activate Payload</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x49</td>
<td>Deactivate Payload</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4A</td>
<td>Get Payload Activation Status</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4B</td>
<td>Get Payload Instance Info</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4C</td>
<td>Set User Payload Access</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4D</td>
<td>Get User Payload Access</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4E</td>
<td>Get Channel Payload Support</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4F</td>
<td>Get Channel Payload Version</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x50</td>
<td>Get Channel OEM Payload Info</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x54</td>
<td>Get Channel Cipher Suites</td>
<td>Supported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x55</td>
<td>Suspend/Resume Payload Encryption</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x56</td>
<td>Set Channel Security Keys</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x06</td>
<td>0x57</td>
<td>Get System Interface Capabilities</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>
## Chassis commands

### Chassis device commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Get Chassis Capabilities</td>
<td>Supported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x01</td>
<td>Get Chassis Status</td>
<td>Supported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x02</td>
<td>Chassis Control</td>
<td>Supported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x04</td>
<td>Chassis Identify</td>
<td>Supported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x05</td>
<td>Set Chassis Capabilities</td>
<td>Supported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x06</td>
<td>Set Power Restore Policy</td>
<td>Supported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x07</td>
<td>Get System Restart Cause</td>
<td>Unsupported*</td>
</tr>
<tr>
<td>0x00</td>
<td>0x08</td>
<td>Set System Boot Options</td>
<td>Supported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x09</td>
<td>Set System Boot Options</td>
<td>Supported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x0A</td>
<td>Set Front Panel Button Enables</td>
<td>Unsupported*</td>
</tr>
<tr>
<td>0x00</td>
<td>0x0B</td>
<td>Set Power Cycle Interval</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x00</td>
<td>0x0F</td>
<td>Get PDH Counter</td>
<td>Unsupported*</td>
</tr>
</tbody>
</table>
| * Commands are not rejected and can cause unpredictable behavior.

## Bridge commands

### Bridge management commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>0x00</td>
<td>Get Bridge State</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x01</td>
<td>Set Bridge State</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x02</td>
<td>Get ICMB Address</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x03</td>
<td>Set ICMB Address</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x04</td>
<td>Set Bridge Proxy Address</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x05</td>
<td>Get Bridge Statistics</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x06</td>
<td>Get ICMB Capabilities</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x08</td>
<td>Clear Bridge Statistics</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x09</td>
<td>Get Bridge Proxy Address</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x0A</td>
<td>Get ICMB Connector Info</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>

### Bridge discovery commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>0x10</td>
<td>Prepare For Discovery</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x11</td>
<td>Get Addresses</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x12</td>
<td>Set Discovered</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x13</td>
<td>Get Chassis Device Id</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x14</td>
<td>Set Chassis Device Id</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>

### Bridging commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>0x20</td>
<td>Bridge Request</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x21</td>
<td>Bridge Message</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>

### Bridge event commands
<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>0x30</td>
<td>Get Event Count</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x31</td>
<td>Set Event Destination</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x32</td>
<td>Set Event Reception State</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x33</td>
<td>Send ICMB Event Message</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x34</td>
<td>Get Event Destination</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x02</td>
<td>0x35</td>
<td>Get Event Reception State</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>

**Sensor event commands**

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

**Storage commands**

**FRU information commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0a</td>
<td>0x10</td>
<td>Get FRU Inventory Area Info</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x11</td>
<td>Read FRU Data</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x12</td>
<td>Write FRU Data</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**SDR repository commands**
<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0a</td>
<td>0x20</td>
<td>Get SDR Repository Info</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x21</td>
<td>Get SDR Repository Allocation Info</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x22</td>
<td>Reserve SDR Repository</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x23</td>
<td>Get SDR</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x24</td>
<td>Add SDR</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x25</td>
<td>Partial Add SDR</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x27</td>
<td>Clear SDR Repository</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x28</td>
<td>Get SDR Repository Time</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x2C</td>
<td>Run Initialization Agent</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x26</td>
<td>Delete SDR Repository</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>

**SEL device commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0a</td>
<td>0x40</td>
<td>Get SEL Info</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x41</td>
<td>Get SEL Allocation Info</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x42</td>
<td>Reserve SEL</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x43</td>
<td>Get SEL Entry</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x44</td>
<td>Add SEL Entry</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x45</td>
<td>Partial Add SEL Entry</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x46</td>
<td>Delete SEL Entry</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x47</td>
<td>Clear SEL</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x48</td>
<td>Get SEL Time</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x49</td>
<td>Set SEL Time</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x5C</td>
<td>Get SEL Time UTC Offset</td>
<td>Unsupported</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x5D</td>
<td>Set SEL Time UTC Offset</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>

**Transport commands**

**LAN device commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0C</td>
<td>0x01</td>
<td>Set LAN Configuration Parameters</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0C</td>
<td>0x02</td>
<td>Get LAN Configuration Parameters</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0C</td>
<td>0x03</td>
<td>Suspend BMC ARPs</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>

**Serial over LAN commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0C</td>
<td>0x22</td>
<td>Get SOL Configuration Parameters</td>
<td>Supported</td>
</tr>
<tr>
<td>0x0C</td>
<td>0x21</td>
<td>Set SOL Configuration Parameters</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**Kontron OEM commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x3C</td>
<td>0x07</td>
<td>UEFI Recovery</td>
<td>Supported</td>
</tr>
</tbody>
</table>
Document symbols and acronyms

Symbols

The following symbols are used in Kontron documentation:

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

<table>
<thead>
<tr>
<th>Electric Shock!</th>
</tr>
</thead>
<tbody>
<tr>
<td>This symbol and title warn of hazards due to electrical shocks (&gt; 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 &quot;High-Voltage Safety Instructions&quot; portion below in this section.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESD Sensitive Device!</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HOT Surface!</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do NOT touch! Allow to cool before servicing.</td>
</tr>
</tbody>
</table>

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

| This symbol precedes helpful hints and tips for daily use. |

Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACPI</td>
<td>Advanced Configuration and Power Interface</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
</tr>
<tr>
<td>BMC</td>
<td>Baseboard Management Controller</td>
</tr>
<tr>
<td>BSP</td>
<td>Board Support Package</td>
</tr>
<tr>
<td>CBIT</td>
<td>Continuous Built-In Test</td>
</tr>
<tr>
<td>CE</td>
<td>Community European (EU mark)</td>
</tr>
<tr>
<td>CLI</td>
<td>Command-Line Interface</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRMS</td>
<td>Communications Rack Mount Servers</td>
</tr>
<tr>
<td>CSA</td>
<td>Canadian Standards Association</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>DDR4</td>
<td>Double Data Rate Fourth Generation</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DIMM</td>
<td>Dual Inline Memory Module</td>
</tr>
<tr>
<td>DRAM</td>
<td>Dynamic Random Access Memory</td>
</tr>
<tr>
<td>DTS</td>
<td>Digital Thermal Sensor</td>
</tr>
<tr>
<td>DU</td>
<td>Distributed Unit</td>
</tr>
<tr>
<td>ECC</td>
<td>Error Checking and Correcting</td>
</tr>
<tr>
<td>EEPROM</td>
<td>Electrically Erasable Programmable Read-Only Memory</td>
</tr>
<tr>
<td>EMC</td>
<td>Electromagnetic Compatibility</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>ESD</td>
<td>Electrostatic Discharge</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>eUSB</td>
<td>Embedded Universal Serial Bus</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FH/FL</td>
<td>Full Height/Full Length</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
</tr>
<tr>
<td>FRAU</td>
<td>Field Replaceable Unit</td>
</tr>
<tr>
<td>FRU</td>
<td>Field Replaceable Unit</td>
</tr>
<tr>
<td>Gb, Gbit</td>
<td>Ggabit</td>
</tr>
<tr>
<td>GB, Gbyte</td>
<td>Ggabyte – 1024 MB</td>
</tr>
<tr>
<td>GbE</td>
<td>Ggabit Ethernet</td>
</tr>
<tr>
<td>GND</td>
<td>Ground</td>
</tr>
<tr>
<td>GPI</td>
<td>General Purpose Input</td>
</tr>
<tr>
<td>GPIO</td>
<td>General Purpose Input/Output</td>
</tr>
<tr>
<td>GPO</td>
<td>General Purpose Output</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>Hz</td>
<td>Hertz – 1 cycle/second</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>I 2 C</td>
<td>Inter-Integrated Circuit Bus</td>
</tr>
<tr>
<td>iBMC</td>
<td>Integrated Baseboard Management Controller</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IMU</td>
<td>Inertial Measurement Unit</td>
</tr>
<tr>
<td>IOL</td>
<td>IPMI over LAN</td>
</tr>
<tr>
<td>iPMB</td>
<td>Intelligent Platform Management Bus</td>
</tr>
<tr>
<td>IPMI</td>
<td>Intelligent Platform Management Interface</td>
</tr>
<tr>
<td>IRQ</td>
<td>Interrupt Request Line</td>
</tr>
<tr>
<td>KB, Kbyte</td>
<td>Kilobyte – 1024 bytes</td>
</tr>
<tr>
<td>KCS</td>
<td>Keyboard Controller Style</td>
</tr>
<tr>
<td>KEAPI</td>
<td>Kontron Embedded Application Programming Interface</td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard, Video, Mouse</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LED</td>
<td>Light-Emitting Diode</td>
</tr>
<tr>
<td>LP</td>
<td>Low Profile</td>
</tr>
<tr>
<td>LPC</td>
<td>Low Pin Count</td>
</tr>
<tr>
<td>LVDS</td>
<td>Low Voltage Differential SCSI</td>
</tr>
<tr>
<td>MAT</td>
<td>Maximum Ambient Temperature</td>
</tr>
<tr>
<td>MB, Mbyte</td>
<td>Megabyte – 1024 KB</td>
</tr>
<tr>
<td>MCU</td>
<td>Microcontroller</td>
</tr>
<tr>
<td>MEC</td>
<td>Multi-Access Edge Computing</td>
</tr>
<tr>
<td>MXM</td>
<td>Mobile PCI Express Module</td>
</tr>
<tr>
<td>NCSI</td>
<td>Network Communications Services Interface</td>
</tr>
<tr>
<td>NEBS</td>
<td>Network Equipment-Building System</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card, or Network Interface Controller, or Network Interface Controller port</td>
</tr>
<tr>
<td>NMI</td>
<td>Non-Maskable interrupt</td>
</tr>
<tr>
<td>NOS</td>
<td>Network Operating System</td>
</tr>
<tr>
<td>NVMe</td>
<td>Non-Volatile Memory Express</td>
</tr>
<tr>
<td>OCKO</td>
<td>Oven-Controlled Crystal Oscillator</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OTP</td>
<td>Over-Temperature Protection</td>
</tr>
<tr>
<td>OVP</td>
<td>Over-Voltage Protection</td>
</tr>
<tr>
<td>PBIT</td>
<td>Power On Built-In Test</td>
</tr>
<tr>
<td>PCH</td>
<td>Platform Controller Hub</td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
</tr>
<tr>
<td>PCIe</td>
<td>Peripheral Component Interconnect Express</td>
</tr>
<tr>
<td>PECI</td>
<td>Platform Environment Control Interface</td>
</tr>
<tr>
<td>PIIRQ</td>
<td>PCI Interrupt Request Line</td>
</tr>
<tr>
<td>PMbus</td>
<td>Power Management Bus</td>
</tr>
<tr>
<td>PMM</td>
<td>POST Memory Manager</td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>POST</td>
<td>Power-On Self Test</td>
</tr>
<tr>
<td>PSU</td>
<td>Power Supply Unit</td>
</tr>
<tr>
<td>PTP</td>
<td>Precision Time Protocol</td>
</tr>
<tr>
<td>PXE</td>
<td>Preboot eXecution Environment</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>RAS</td>
<td>Reliability, Availability, and Serviceability</td>
</tr>
<tr>
<td>RDIMM</td>
<td>Registered Dual In-Line Memory Module</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop</td>
</tr>
<tr>
<td>RMM</td>
<td>Remote Management Module</td>
</tr>
<tr>
<td>RoHS</td>
<td>Restriction of Hazardous Substances</td>
</tr>
<tr>
<td>SAS</td>
<td>Serial Attached SCSI (Small Computer System Interface)</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial Advanced Technology Attachment</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small Computer Systems Interface</td>
</tr>
<tr>
<td>SDRAM</td>
<td>Synchronous Dynamic RAM</td>
</tr>
<tr>
<td>SEL</td>
<td>System Event Log</td>
</tr>
<tr>
<td>SFP+</td>
<td>Small Form-factor Pluggable that supports data rates up to 10.0 Gbps</td>
</tr>
<tr>
<td>SMBus</td>
<td>System Management Bus</td>
</tr>
<tr>
<td>SMS</td>
<td>Server Management Software</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOC</td>
<td>System on a Chip</td>
</tr>
<tr>
<td>SOL</td>
<td>Serial over LAN</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>THOL</td>
<td>Tested Hardware and Operating System List</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>TUV</td>
<td>Technischer Überwachungs-Verein (A safety testing laboratory with headquarters in Germany)</td>
</tr>
<tr>
<td>UART</td>
<td>Universal Asynchronous Receiver Transmitter</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>UL</td>
<td>Underwriter’s Laboratory</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>UV</td>
<td>Under-Voltage</td>
</tr>
<tr>
<td>V</td>
<td>Volt</td>
</tr>
<tr>
<td>VA</td>
<td>Volt-Ampere (volts multiplied by amps)</td>
</tr>
<tr>
<td>Vac</td>
<td>Volts Alternating Current</td>
</tr>
<tr>
<td>Vdc</td>
<td>Volts Direct Current</td>
</tr>
<tr>
<td>VDE</td>
<td>Verband Deutscher Electrotechniker (German Institute of Electrical Engineers)</td>
</tr>
<tr>
<td>VGA</td>
<td>Video Graphics Array</td>
</tr>
<tr>
<td>vRAN</td>
<td>Virtualized Radio Access Network</td>
</tr>
<tr>
<td>VSB</td>
<td>Voltage Standby</td>
</tr>
<tr>
<td>W</td>
<td>Watt</td>
</tr>
<tr>
<td>WEEE</td>
<td>Waste Electrical and Electronic Equipment</td>
</tr>
<tr>
<td>Ω</td>
<td>Ohm</td>
</tr>
</tbody>
</table>