

# User Documentation - ME1100

POSSIBILITIES START HERE  kontron



# Table of Content

- [User Documentation - ME1100](#)
  - [Product description](#)
  - [Overview](#)
    - [Specifications](#)
    - [Platform components](#)
    - [Product architecture](#)
    - [Description of system access methods](#)
    - [Recommended technical expertise](#)
  - [Getting started](#)
    - [Getting started - Application installation and performance benchmarking](#)
  - [Planning](#)
    - [Environmental considerations](#)
    - [Power consumption and power budget](#)
    - [Network architecture](#)
    - [MAC addresses](#)
    - [PCI mapping](#)
    - [Platform modules and accessories](#)
    - [Material, information and software required](#)
    - [Hardware compatibility list](#)
    - [Validated operating systems](#)
    - [Security](#)
  - [Installing](#)
    - [Mechanical installation and precautions](#)
      - [ESD protections](#)
      - [Unboxing](#)
      - [Component installation and assembly](#)
      - [Airflow](#)
      - [Rack installation](#)
      - [Cabling](#)
    - [Software installation and deployment](#)
      - [Preparing for installation](#)
      - [Installing an operating system on a server](#)
      - [Verifying installation](#)
      - [Common software installation](#)
  - [Configuring](#)
    - [Configuring system access methods](#)
    - [Configuring and managing users](#)
    - [Baseboard management controller - BMC](#)
    - [Configuring the network time protocol - NTP](#)
    - [Basic BIOS option configuration](#)
  - [Operating](#)
    - [Default user names and passwords](#)
    - [Accessing platform components](#)
      - [Accessing the operating system of a server](#)
      - [Accessing the BIOS](#)
      - [Accessing a BMC on an ME1100](#)
    - [Platform power management](#)
    - [Monitoring](#)
      - [Monitoring sensors](#)
      - [Sensor list](#)
      - [Interpreting sensor data](#)
      - [Managing customer added sensors](#)
    - [Maintenance](#)
      - [System event log](#)
      - [Component replacement](#)
      - [Upgrading](#)

# PRELIMINARY

- [Platform cooling and thermal management](#)
- [Application ready indication via power LED](#)
- [Troubleshooting](#)
  - [Collecting diagnostics](#)
  - [Factory default](#)
    - [\(WiP\) - Restoring Default BIOS Settings Using the JP1 Connector](#)
  - [Support information](#)
- [Reference guides](#)
  - [Supported IPMI commands](#)
- [Document symbols and acronyms](#)
- [Safety and regulatory information](#)
- [Warranty and support](#)

## Product description

*{This article briefly describes the physical product, features and main options.}*

Table of contents

- [ME1100 platform](#)
  - [Main applications](#)
  - [Main features](#)

## ME1100 platform



The goal of multi-access edge computing is to decrease network congestion and improve the performance of applications or workloads by getting task processing closer to the user.

Our mobile edge Xeon® D servers enable content and applications to reside closer to the edge. This allows operators to solve challenges related to restricted space and power while reducing overall costs. The ME1100 1U platform enables edge applications based on Radio Access Network, artificial intelligence, data caching, ultra-low latency and high-bandwidth, among others.

### Main applications

- High-performance server for multi-access edge computing (MEC)
- Enabling IT and cloud-computing capabilities within the Radio Access Network (RAN)
- Ideal for ultra-low latency and high-bandwidth applications
- Storage and extension slot for artificial intelligence or data caching applications

### Main features

- Extended operating temperature range: -40°C to 65°C
- 19-in 1U rackmount, 300-mm deep
- Intel® Xeon® D-1500 processor series (8C, 12C)
- Two embedded 10 GbE SFP network interfaces
- One FHHL or FH3/4L PCIe add-in card

## Overview

Children

- [Specifications](#)
- [Platform components](#)
- [Product architecture](#)
- [Description of system access methods](#)
- [Recommended technical expertise](#)

## Specifications

{This article details dimensions, shipping weights, environmental specifications and power consumption and lists key hardware and software features.}

Table of contents

- [ME1100 key hardware features](#)
- [ME1100 key software features](#)
- [ME1100 physical dimensions](#)
- [ME1100 packaging physical dimensions](#)
- [ME1100 shipping weights](#)
- [ME1100 environmental specifications](#)

**ME1100 key hardware features**

## PRELIMINARY

Feature	Description
Hardware platform	<ul style="list-style-type: none"> <li>• High-performance server for mobile edge computing (MEC), 1U height, 300-mm deep, 19 inches wide</li> <li>• Hot-swappable fan tray and filter</li> <li>• Front access only (motherboard I/O, PSU, PCIe add-in card I/O, fan tray)</li> </ul>
I/O	<ul style="list-style-type: none"> <li>• Two 10 GbE SFP+</li> <li>• One USB 2.0</li> <li>• One RJ45 10/100/1000Base-T management port</li> <li>• One RJ45 serial port</li> <li>• One reset button</li> </ul>
PCIe add-in card	<ul style="list-style-type: none"> <li>• One optional FHHL or FH<math>\frac{3}{4}</math>L PCIe x16 add-in card supported (power and thermal restrictions may apply)</li> <li>• Maximum power consumption supported is 50 W</li> </ul> <p>Refer to the <a href="#">Hardware compatibility list</a></p>
CPU	<p>Intel® Xeon® D-1500 family processors are supported, including the following processors:</p> <ul style="list-style-type: none"> <li>• Xeon® D-1548, 8 Cores @ 2.00GHz, 45W</li> <li>• Xeon® D-1567, 12 Cores @ 2.10GHz, 65W</li> <li>• Xeon® D-1559, 12 Cores @ 1.50GHz, 45W</li> </ul>
Drive	<p>One M.2 SATA SSD up to 2280 option:</p> <ul style="list-style-type: none"> <li>• Refer to the <a href="#">Hardware compatibility list</a></li> </ul> <p>Four 2.5-in SATA SSD option:</p> <ul style="list-style-type: none"> <li>• Refer to the <a href="#">Hardware compatibility list</a></li> </ul>
Memory	<p>DDR4 DIMM with ECC</p> <ul style="list-style-type: none"> <li>• Bandwidth up to 2400 MT/s</li> <li>• Two memory channels</li> <li>• One DIMM socket per channel</li> </ul> <p>Refer to the <a href="#">Hardware compatibility list</a></p>
Power inlet	<p>One optional -57 VDC to -40 VDC dual input feed or 90 VAC to 265 VAC single Input</p>
Power consumption	Refer to <a href="#">Power consumption and power budget</a>
Fans	<p>Hot-swappable fan tray:</p> <ul style="list-style-type: none"> <li>• Fan tray contains 3 fans (standard configuration)</li> <li>• Fan tray contains 4 fans when 2.5-in SATA SSD option is installed</li> <li>• Fan filter can be removed independently from the fan tray</li> <li>• Automatic fan speed control</li> </ul>
Rack mounting brackets	Front or middle mount in a 19-in wide rack

### ME1100 key software features

# PRELIMINARY

Feature	Description
Platform management	<ul style="list-style-type: none"> <li>• Integrated BMC – this subsystem consists of communication buses, sensors, system BIOS, and server management firmware; it supports standard IPMI features as well as OEM (supplemental) features that are not part of IPMI</li> <li>• IPMI-based system monitor used for server monitoring, diagnostic and configuration</li> <li>• System event log</li> <li>• Server power consumption monitoring</li> <li>• Server power control</li> <li>• Server and component health monitoring</li> <li>• Fan speed monitoring</li> <li>• Serial over LAN console access</li> <li>• IPMI over LAN</li> <li>• Sensor data record describing all sensors and providing their readings (analog or discrete)</li> <li>• ACPI state synchronization: the BMC tracks ACPI state changes that are provided by the BIOS</li> <li>• BIOS recovery</li> </ul>
Operating system	Refer to the <a href="#">Validated operating systems</a>
Thermal management	<ul style="list-style-type: none"> <li>• Platform Environment Control Interface (PECI) for thermal management support</li> <li>• Memory and CPU thermal management</li> </ul>

## ME1100 physical dimensions

Chassis	Measurements (mm [in])	Notes
Depth	300 [11.8]	Body
Width	449 [17.6] max.	Body
	483 [19] max.	Overall width: front mounting brackets included (2 times 17.2 mm [0.7 in])
	465 [18.3]	Between rack mounting points
Height	43.5 [1.7] max.	Body
Side clearance	70 [2.8]	Between rack mounting points
Front clearance	100 [4]	Recommended
Rear clearance	None	

## ME1100 packaging physical dimensions

Depth (mm [in])	Width (mm [in])	Height (mm [in])
422 [16.6]	605 [23.8]	170 [6.7]

## ME1100 shipping weights

Component	Weight (kg)	Weight (lb)
System weight – with two DIMM and one M.2-2280 SATA SSD	4.37	9.63
Packaging (box + foam + bag)	1.124	2.48
2.5-in SSD carrier bracket	0.206	0.45
2.5-in SATA SSD (1)	0.060	0.13

# PRELIMINARY

## ME1100 environmental specifications

Environment	Specification
Temperature, operating	<p>-40°C to +65°C (-40°F to +149°F)</p> <p>The failure of one fan will not impact operation for at least 4 hours at 65°C.</p> <p>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 recommends using SFP+ and SSD modules with an industrial operating temperature range (-40°C to +85°C). Another limitation can result from airflow obstruction caused by fan filter clogging and failure to follow recommended side clearances.</p>
Temperature, non-operating	-40°C to +70°C (-40°F to +158°F)
Humidity, operating	5% to 95%, non-condensing
Altitude/pressure, operating	<p>-60 m to 1,800 m altitude without temperature de-rating</p> <p>Up to 4,000 m altitude with temperature de-rating of 1 degree Celsius per 300 m above 1,800 m</p>
Altitude/pressure, non-operating	Up to 4,570 m
Vibration, operating	<p>This product meets operational random vibration</p> <p>Test profile based on ETSI EN 300 019-2-3 class 3.2</p> <ul style="list-style-type: none"> <li>• 5 Hz to 10 Hz at +12 dB/octave (slope up)</li> <li>• 10 Hz to 50 Hz at 0.02 m<sup>2</sup>/s<sup>3</sup> (0.0002 g<sup>2</sup>/Hz) (flat)</li> <li>• 50 Hz to 100 Hz at -12 dB/octave (slope down)</li> <li>• 30 minutes for each of the three axes</li> </ul>
Vibration, non-operating	<p>This product meets transportation and storage random vibration</p> <p>Test profile based on GR-63 clause 5.4.3, and ETSI EN 300 019-2-2 class 2.3</p> <ul style="list-style-type: none"> <li>• 5 Hz to 20 Hz at 1 m<sup>2</sup>/s<sup>3</sup> (0.01 g<sup>2</sup>/Hz) (flat)</li> <li>• 20 Hz to 200 Hz at -3 dB/octave (slope down)</li> <li>• 30 minutes for each of the three axes</li> </ul>
Shock, operating	<p>This product meets operational shock standards</p> <p>Test profile based on ETSI EN 300 019-2-3 class 3.2</p> <ul style="list-style-type: none"> <li>• 11 ms half sine, 3 g, three shocks in each direction</li> </ul>
Drop/free fall	<p>This product meets Bellcore GR-63 section 5.3</p> <p>Packaged = 1,000 mm, six surfaces, three edges and four corners</p> <p>Unpackaged = 100 mm, two sides and two bottom corners</p>
Electrostatic discharge	This product meets 8 kV contact, 15 kV air discharge using IEC 61000-4-2 test method
RoHS and WEEE	<p>This product is designed to meet China RoHS Phase 1 (self-declaration and labeling)</p> <p>This product complies with EU directive 2012/19/EU (WEEE)</p> <p>This product complies with RoHS directive 2011/65/EU as modified by EU 2015/863</p>

# Platform components

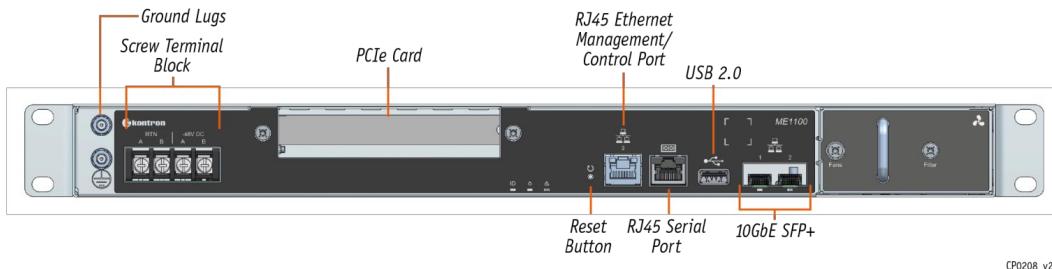
{This article describes the platform's various components: panels, LEDs, modules, fans and power supply units.}

Table of contents

- [Platform front panel](#)
  - [DC](#)
  - [AC](#)
  - [Platform LEDs](#)
  - [Management/control plane port LEDs](#)
  - [Network port LEDs](#)
  - [Serial port connector pinout](#)
- [Fans and filter](#)

## Platform front panel

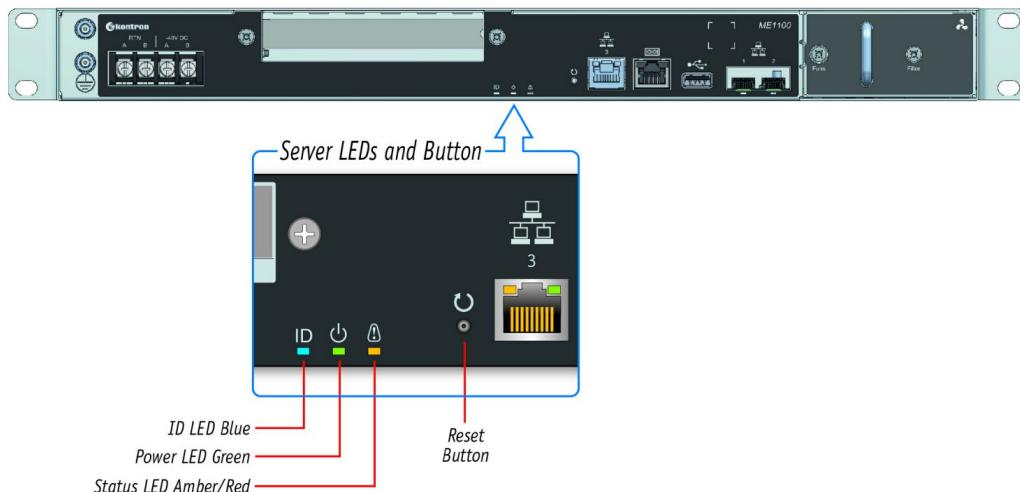
DC



AC



## Platform LEDs



## PRELIMINARY

ID (blue)	Power (green)	State
Off	Off	Both power inputs DOWN or out of range for normal operation
On	Off	One or both power inputs UP – ACPI Software off state (S5)
Slow blink	Off	Platform preheating prior to server activation
Normal blink	Any	BMC is executing an identification request
Off	Rapid blink	Server processor activation complete and executing – ACPI Working state (S0)
Off	Normal blink	BIOS started POST
Off	Normal blink or On <sup>1</sup>	BIOS hand over to OS boot loader
Off	On <sup>1</sup>	Application started/running OK

<sup>1</sup> By default, the Power LED will "normal blink" until customer application confirms it is running by setting an I/O register bit. Via a BIOS setting, the Power LED can be set to steady on after POST (before starting the OS/application), but the default BIOS setting leaves that task to the application.

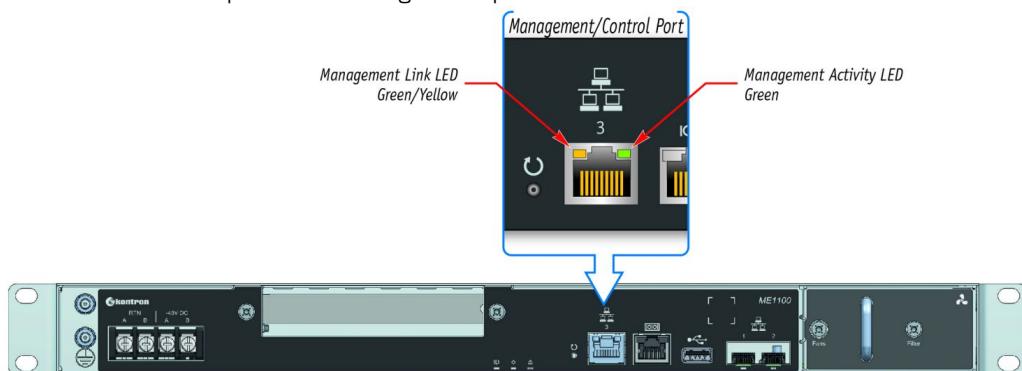
- Slow blink: 1 short pulse every 2 seconds
- Normal blink: 1 pulse every second
- Rapid blink: 2 pulses every second

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

Button state	Behavior
Reset button pressed	CPU resets (does not affect the management controller)

### Management/control plane port LEDs

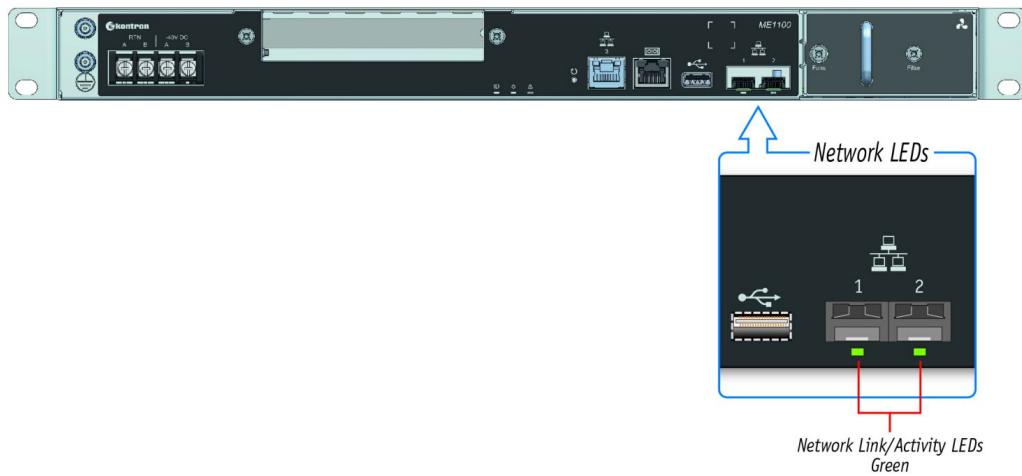
Port number 3 is the platform management port.



# PRELIMINARY

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

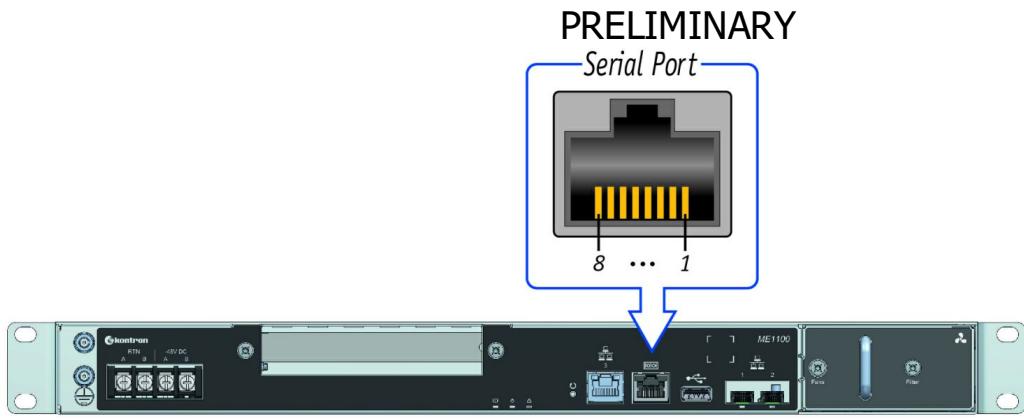
## Network port LEDs



CP0283

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

## Serial port connector pinout



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

CP0209\_v2

## Fans and filter

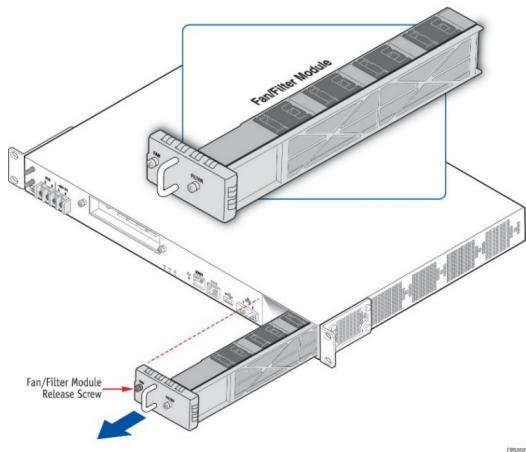
The ME1100 platform is equipped with a fan tray assembly comprised of fans and a filter. The filter can be pulled out by itself or the entire fan tray assembly (i.e., the fans and the filter) can be pulled out.

- To service the entire fan tray: unfasten the fan screw.
- To service the filter only: unfasten the filter screw and clean using oil-free compressed air.

<b>WARNING</b>	Always replace the fan tray with the equivalent fan tray assembly (part number). Two fan tray kits are available for the ME1100 product. Fan tray with 3 fans (standard) and fan tray with 4 fans when ME1100 is configured with 2.5-in SSDs. Using the wrong fan tray may cause thermal issues in the system.
<b>WARNING</b>	Fan air filter should be inspected on a regular basis, based on the environment of their location. The inspection could be required every 2 years (in a very clean environment) or even every 3 months (in a slightly dusted environment). It is recommended that 3 months after the first installation, an inspection is executed in order to assess the ?state? of the filter. Base on how the filter is clogged, the schedule for cleaning or replacement of the filter can be established. Note that for installation done according to Telcordia NEBS requirements, filters must be replaced (R4-27 [145]) they cannot be cleaned. For other type of installation, filters could be cleaned up to 3 times, after what they must be replaced. It is recommended to replace filter every 3 years, replacement is required before residual dust build-up and provide air flow resistance. To clean filter you can use slightly compressed air, vacuum, and/or rinsed them with clean water. If water is use make sure the filter is completely dry before reinstalling

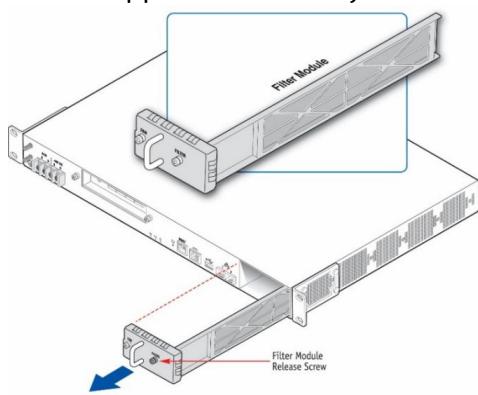
## Hot-swappable fan tray

# PRELIMINARY



CP0202

Hot-swappable filter tray



CP0203

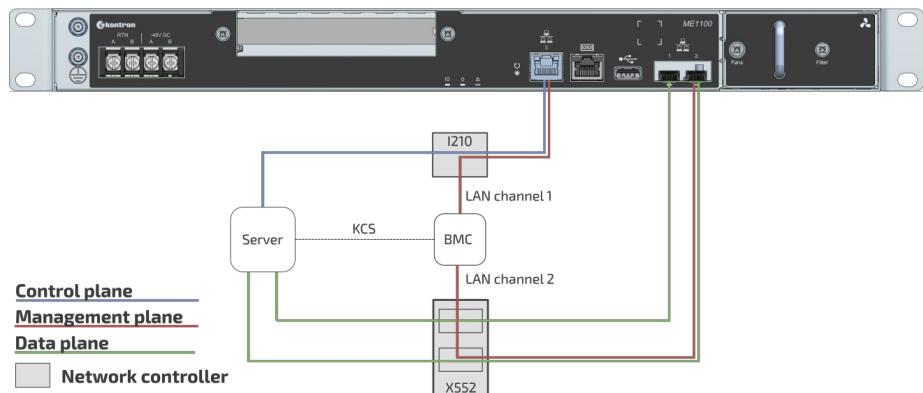
# Product architecture

*(This article provides visual representations of the system's architecture and network interconnections as well as block diagrams.)*

Table of contents

- [Internal connections](#)
- [Network planes](#)
- [Block diagram](#)

## Internal connections



## Network planes

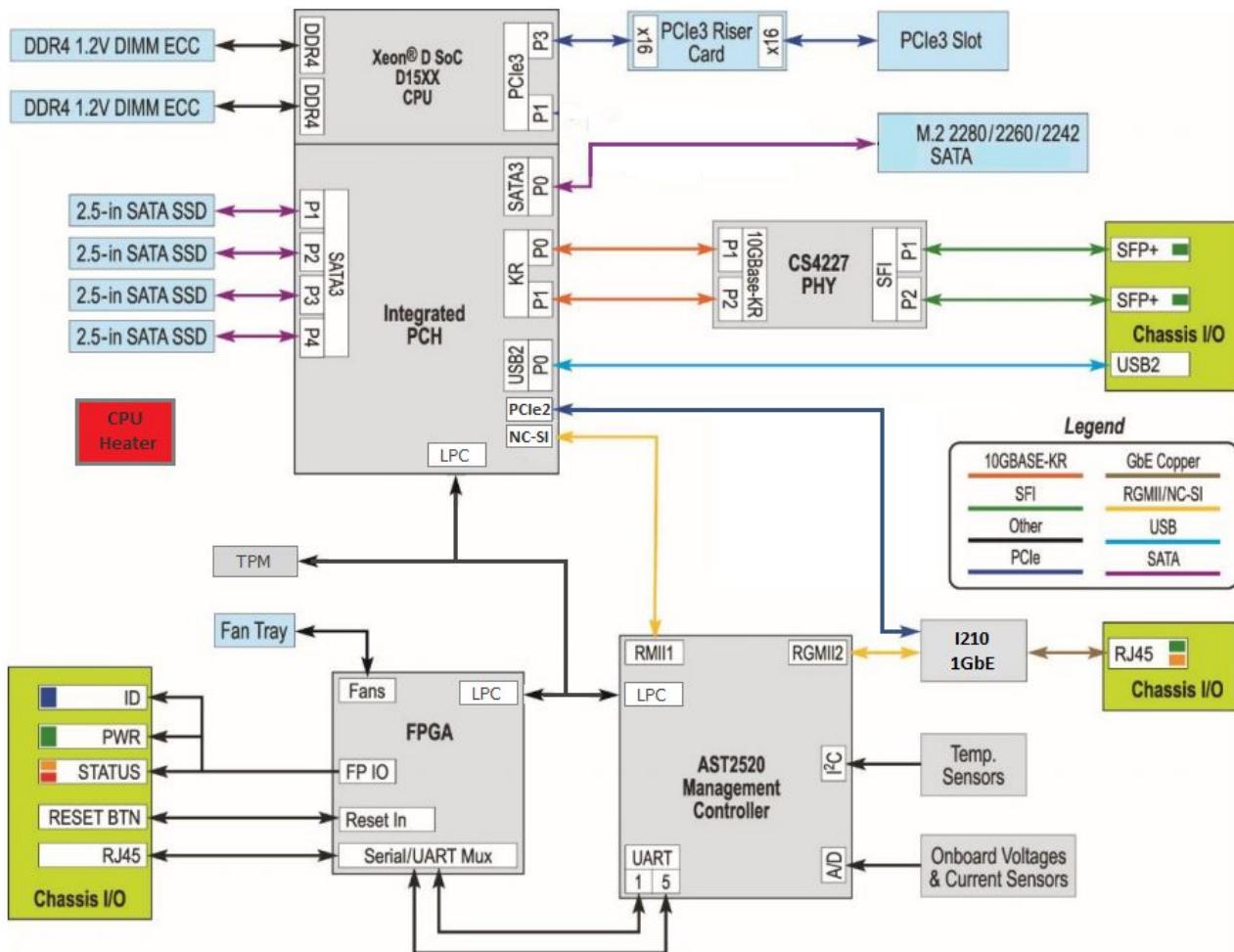
The ME1100 platform provides 3 network planes.

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

## Block diagram

# PRELIMINARY

This block diagram summarizes the connections within the platform.



## Description of system access methods

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

### Table of contents

- [Paths to the operating system](#)
- [Paths to the BIOS](#)
- [Paths to the management interface \(BMC\)](#)

To configure, monitor and troubleshoot the ME1100 platform and its components, several interfaces can be used:

- **Operating system** – through the management plane, control plane, data plane or the serial port of the platform
- **BIOS** – through the management plane or the serial port of the platform
- **Management interface (BMC)** – through the management plane and the data plane of the platform

**NOTE:** The management plane and the control plane of the ME1100 platform are physically accessible through the front RJ45 connector.

## Paths to the operating system

To access the operating system through one of the paths, refer to [Accessing the operating system of a server](#).

Paths to the operating system	
Path description	Main reasons for use
<b>KVM</b> <i>This is the recommended path for first time out-of-the-box system configuration.</i> <i>Fail-safe path to access the server if any elements (OS, BIOS, etc.) get misconfigured.</i> <i>Accessible from the management plane.</i>	<ul style="list-style-type: none"> <li>• Initial OS installation</li> <li>• OS network interface configuration</li> <li>• OS video access</li> <li>• Remote access to the OS</li> <li>• Unable to establish an SSH session to the OS</li> </ul>
<b>SSH/RDP/Customer application protocols</b> <i>Ideal path once OS installation and OS network interface configurations have been performed.</i> <i>Accessible from the control plane and the data plane.</i>	<ul style="list-style-type: none"> <li>• Operating the platform under normal operation</li> <li>• Remote access to the OS</li> </ul>
<b>Serial over LAN (SOL)</b> <i>Accessible from the management plane.</i>	<ul style="list-style-type: none"> <li>• OS network interface configuration</li> <li>• Unable to establish an SSH session to the OS</li> <li>• OS serial console access</li> </ul>
<b>Serial console (physical connection)</b> <i>Fail-safe path to access all server components when elements (OS, BMC BIOS, etc.) get misconfigured.</i> <i>Accessible from the physical port.</i>	<ul style="list-style-type: none"> <li>• Initial OS network interface configuration</li> <li>• No configuration performed on BMCs</li> <li>• Troubleshooting</li> </ul>

## Paths to the BIOS

To access the BIOS through one of the paths, refer to [Accessing the BIOS](#).

Paths to the BIOS	
Path description	Main reasons for use
<b>KVM</b> <i>This is the recommended path for first time out-of-the-box system configuration.</i> <i>Fail-safe path to access the server if any elements (OS, BIOS, etc.) get misconfigured.</i> <i>Accessible from the management plane.</i>	<ul style="list-style-type: none"> <li>Initial BIOS configuration</li> <li>BIOS video access</li> </ul>
<b>Serial over LAN (SOL)</b> <i>Accessible from the management plane.</i>	<ul style="list-style-type: none"> <li>Initial BIOS configuration</li> <li>BIOS serial console access</li> <li>OS network interfaces not configured, but BMC network access is available</li> </ul>
<b>Serial console (physical connection)</b> <i>Fail-safe path to access all server components when elements (OS, BMC BIOS, etc.) get misconfigured.</i> <i>Accessible from the physical port.</i>	<ul style="list-style-type: none"> <li>Initial BIOS configuration</li> <li>No configuration performed on BMCs</li> <li>Troubleshooting</li> </ul>
<b>Redfish</b> <i>This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.</i> <i>Accessible from the management plane.</i>	<ul style="list-style-type: none"> <li>Basic BIOS configuration</li> </ul>

## Paths to the management interface (BMC)

To access the management interface (BMC) through one of the paths, refer to [Accessing a BMC on an ME1100](#).

Paths to the management interface (BMC)	
Path description	Main reasons for use
<b>BMC Web UI</b> <i>This is the recommended path for first time out-of-the-box system configuration.</i> <i>Accessible from the management plane and data plane.</i>	<ul style="list-style-type: none"> <li>• Remote server control and monitoring</li> <li>• OS video access</li> <li>• Firmware upgrades</li> </ul>
<b>IPMI over LAN (IOL)</b> <i>This is a good path for automated monitoring/control script once the platform has been configured for the first time.</i> <i>Accessible from the management plane and data plane.</i>	<ul style="list-style-type: none"> <li>• Remote server control and monitoring</li> <li>• Firmware upgrades</li> </ul>
<b>IPMI via KCS</b> <i>Accessible from the local operating system.</i>	<ul style="list-style-type: none"> <li>• Local access to the BMC from the operating system for server monitoring</li> <li>• Initial BMC configuration</li> </ul>
<b>Redfish</b> <i>This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.</i> <i>Accessible from the management plane.</i>	<ul style="list-style-type: none"> <li>• Remote server monitoring</li> <li>• Remote server control</li> </ul>
<b>SNMP</b> <i>This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.</i> <i>Accessible from the management plane.</i>	<ul style="list-style-type: none"> <li>• Remote server monitoring</li> <li>• Remote server control</li> </ul>

## Recommended technical expertise

*{This article describes the technical knowledge required to fully leverage the platform capabilities.}*

---

Platforms are networking devices.

It is recommended that you identify the appropriate upstream topology with the help of the IT/network personnel managing the upstream network hardware and configuration. This will facilitate the process down the road.

IP addresses will also need to be assigned based on known MAC addresses, so appropriate IT expertise is required.

## Getting started

Children

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

# Getting started - Application installation and performance benchmarking

*{This article provides step-by-step instructions to get a customer application installed for the first time in a lab environment and to get ready for application performance benchmarking.}*

Table of contents

- [Safety and regulatory](#)
- [Introduction](#)
  - [Assumptions](#)
- [Unboxing the platform](#)
  - [What's in the box](#)
- [Planning](#)
  - [Material and information required](#)
    - [PCIe add-in card](#)
    - [DC Power cables and tooling](#)
    - [Rack installation material](#)
    - [Network cables and modules](#)
    - [Network infrastructure](#)
  - [Software required](#)
- [Installing a PCIe add-in card in an ME1100](#)
  - [Opening the enclosure](#)
  - [Adjusting the PCIe add-in card space length to three-quarter length](#)
  - [Adjusting the PCIe add-in card rear mounting bracket](#)
  - [Connecting the PCIe add-in card](#)
  - [Installing a thermal probe for the PCIe add-in card](#)
    - [Locating the thermal probe connection](#)
    - [Installing the thermal probe](#)
  - [Closing the enclosure](#)
- [Racking the platform](#)
- [Connecting the network cables](#)
- [Building and connecting the DC power cables](#)
  - [Material required](#)
  - [Procedure](#)
- [Confirming network links are established](#)
- [Discovering or configuring the platform management IP address](#)
  - [Accessing the BIOS using a serial console \(physical connection\)](#)
    - [Prerequisites](#)
    - [Port location](#)
    - [Access procedure](#)
  - [Accessing the BMC network configuration menu](#)
  - [Discovering the DHCP management IP address](#)
  - [Configuring a static management IP address](#)
- [Preparing for operating system installation](#)
- [Installing an operating system](#)
  - [Prerequisites](#)
  - [Browser considerations](#)
  - [Connecting to the Web UI of the BMC](#)
  - [Changing the user name and password](#)
  - [Launching the KVM](#)
  - [Mounting the operating system image via virtual media](#)
  - [Accessing the BIOS setup menu](#)
  - [Selecting the boot order from boot override](#)
  - [Completing operating system installation](#)
  - [\(Optional\) Changing the boot order in the BIOS menu](#)
- [Verifying operating system installation](#)

## PRELIMINARY

- [Benchmarking an application](#)
- [Monitoring platform sensors using the Web UI](#)
- [Managing PCIe add-in card temperature for system cooling](#)
  - [Accessing the Web UI](#)
  - [Configuring the PCIe add-in card temperature sensor thresholds](#)

## Safety and regulatory

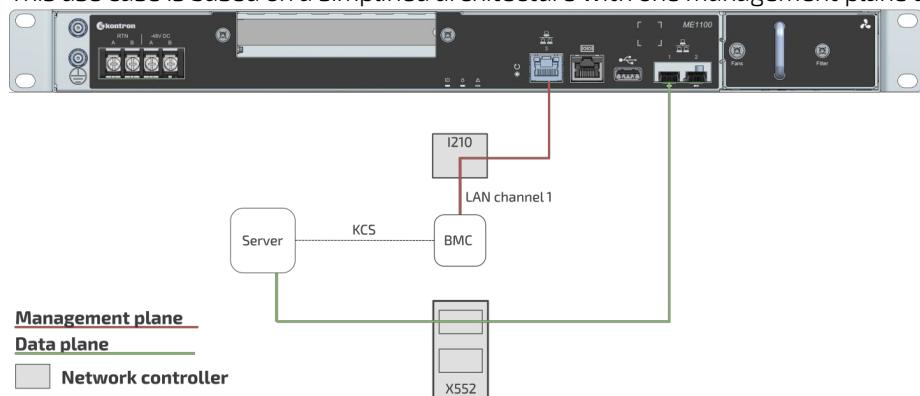
### NOTICE

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 ME1100 platform equipped with one PCIe add-in card provided by the customer and 4 SSD drives and used to leverage two segregated network links (one for the management plane and one for the data plane).

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



To visualize the complete platform architecture or for further details, refer to [Product architecture](#).

## Assumptions

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

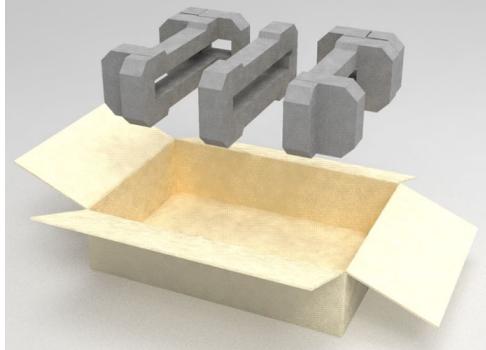
- ME1100 DC input platform
- The network connections of the system are as follows:
  - One management plane (red line) via the RJ45 management port
  - One data plane (green line) via the SFP+ port 1
  - One serial connection via the RJ45 serial port to obtain or configure the BMC management IP address
- The default IPv4 scheme is DHCP, but it can be configured as static in the BIOS setup menu
- The preferred method to obtain or configure the BMC management IP address is through a serial console (physical connection)
- The preferred OS installation method is through the KVM
- The preferred access method is through the Web UI
- PCIe add-in card temperature is monitored using a thermal probe installed in the platform

## Unboxing the platform

### What's in the box

## PRELIMINARY

The ME1100 platform box includes **one** ME1100 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

#### PCIe add-in card

Item_1	One T8 Torx screwdriver
Item_2	One 3-mm flat-head screwdriver
Item_3	One T10 Torx screwdriver
Item_4	One tie wrap, if the PCIe add-in card is a FH3/4L
Item_5	One thermal probe for temperature monitoring (if physical temperature monitoring is chosen)

#### DC Power cables and tooling

## PRELIMINARY

Item_1	Crimp lugs: <ul style="list-style-type: none"> <li>• Two or four Molex insulated spade crimp lugs for 14-16 wire gauge (19131-0023)</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• Two or four Panduit insulated ring crimp lugs for 10-12 wire gauge (EV10-6RB-Q)</li> </ul>
Item_2	Black stranded wire to build the power cable based on the length required: <ul style="list-style-type: none"> <li>• 14 AWG insulation diameter max.: 4.40 mm [0.175 in] for Molex crimp lugs</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• 12 AWG insulation diameter max.: 5.8 mm [0.23 in] for Panduit crimp lugs</li> </ul>
Item_3	Red stranded wire to build the power cable based on the length required: <ul style="list-style-type: none"> <li>• 14 AWG insulation diameter max.: 4.40 mm [0.175 in] for Molex crimp lug</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• 12 AWG insulation diameter max.: 5.8 mm [0.23 in] for Panduit crimp lug</li> </ul>
Item_4	One hand crimp tool: <ul style="list-style-type: none"> <li>• Molex Premium Grade Hand Crimp Tool (640010100)</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• Panduit Hand Crimp Tool (638130400)</li> </ul>
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	8 mm wrench or equivalent tool

### Rack installation material

Item_1	Racking fasteners (rack specific)
--------	-----------------------------------

### Network cables and modules

Relevant section:

[Hardware compatibility list](#)

Item_1	One SFP or SFP+ data plane module and cable <ul style="list-style-type: none"> <li>• SFP/SFP+ optical modules (SX, LX, SR, LR) with compatible optical cable</li> </ul>
Item_2	One RJ45 Ethernet management plane cable
Item_3	One RJ45 serial connection cable

### Network infrastructure

- Two IP addresses:
  - One management plane IP
  - One data plane IP

### Software required

Item_1	A community version of <b>ipmitool</b> is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.
Item_2	A terminal emulator such as <b>puTTY</b> is installed on a remote computer.
Item_3	A hardware detection tool such as <b>pciutils</b> is installed on the local server to view information about devices connected to the server PCI buses .

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

## Installing a PCIe add-in card in an ME1100



### ESD sensitive device!

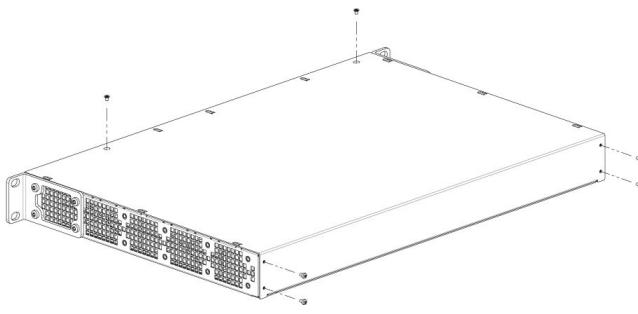
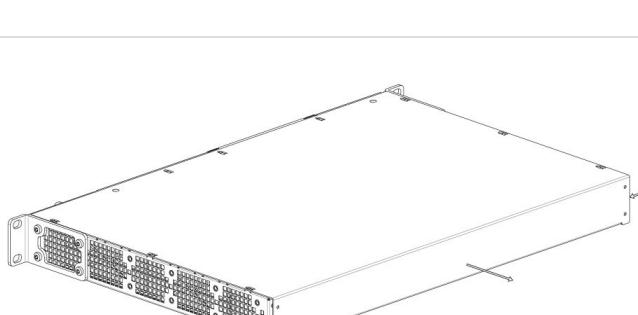
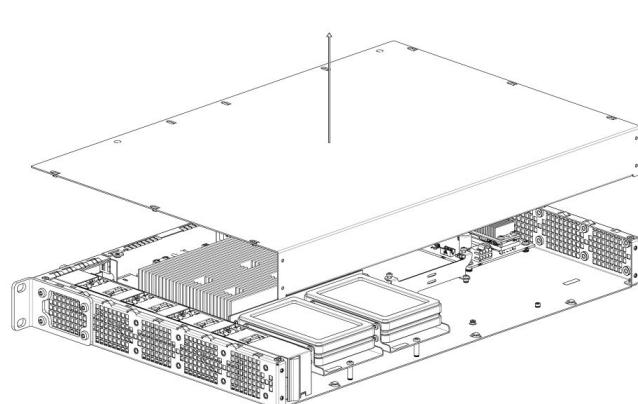
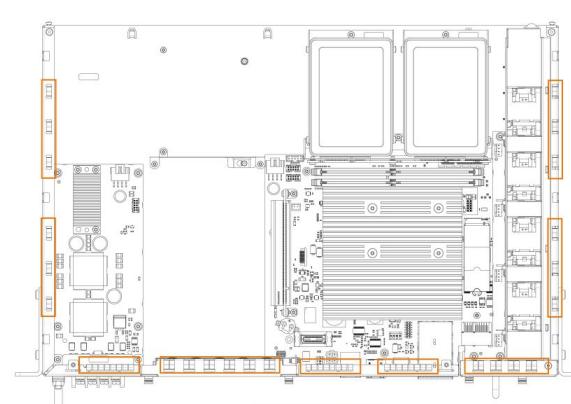
This equipment is sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.



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

### Opening the enclosure

## PRELIMINARY

Step_1	Remove the 4 screws in the back using a T8 Torx screwdriver.	
Step_2	Remove the 2 screws on top using a T8 Torx screwdriver .	
Step_3	On both sides of the unit, insert a flat-head screwdriver in the cavity shown, and slightly slide the cover to the back to release it.	
Step_4	Apply pressure on the cover with your hands to release it from the casing.	
Step_5	Make sure the EMI shield brackets are in their appropriate position. They should not fall in the chassis.	 EMI shield brackets

### Adjusting the PCIe add-in card space length to three-quarter length

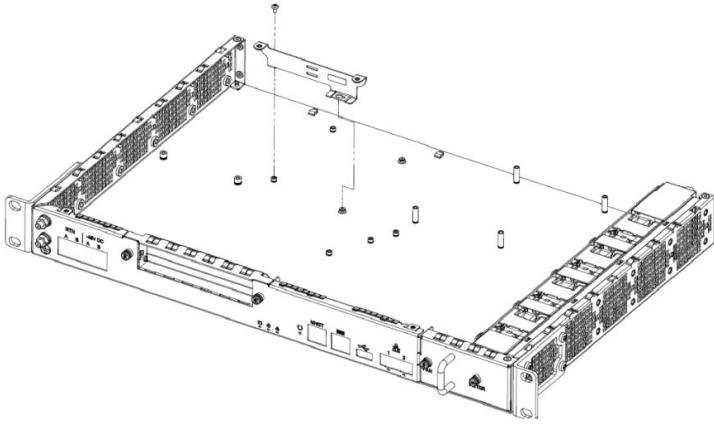
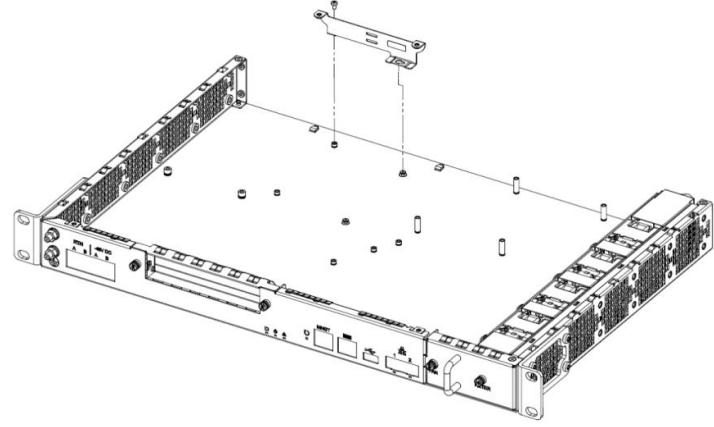
The maximum form factor of the optional PCIe add-in card is full-height, three-quarter length (FH3/4L). T8 and T10 Torx screwdrivers, cutting pliers and a tie wrap are required.

**NOTE:** The unit's default configuration is set for a full-height, half-length ( FHHL ) PCIe add-in card. If your PCIe add-in

# PRELIMINARY

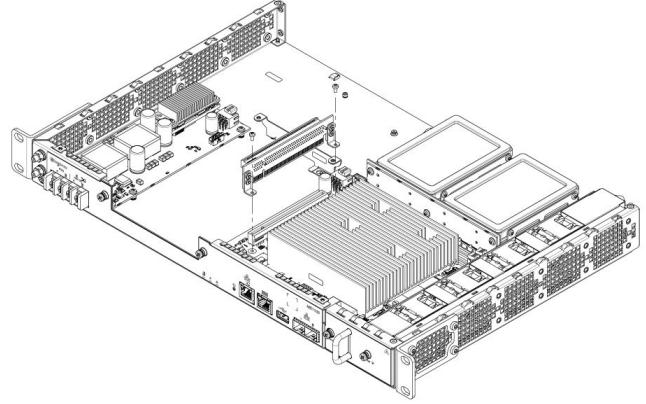
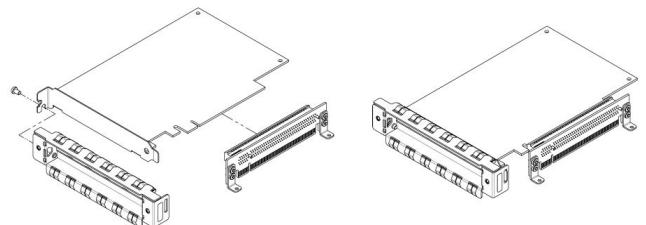
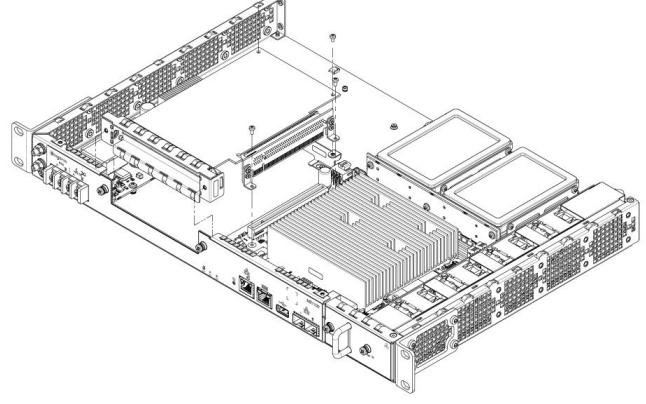
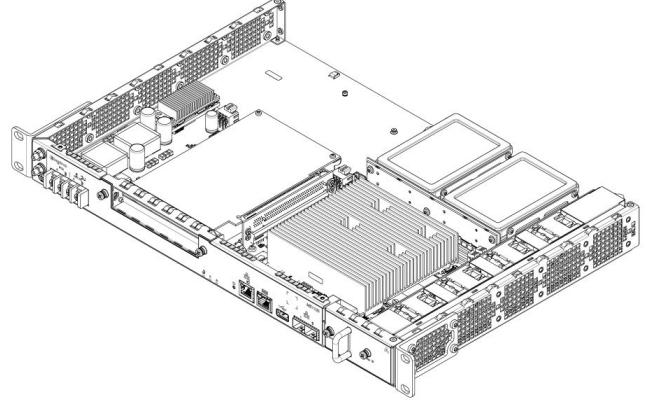
card is FHHL , skip to [Connecting the PCIe add-in card](#).

## Adjusting the PCIe add-in card rear mounting bracket

Step_1	Cut the tie wrap holding the power cable. Be careful not to cut one of the wires.	
Step_2	Remove the PCIe rear mounting bracket from the enclosure by removing the screw with a T8 Torx screwdriver.	
Step_3	Move the PCIe rear mounting bracket to the desired position and fasten the screw with a T8 Torx screwdriver .	
Step_4	Reattach the power cable using a tie wrap as shown in the picture.	

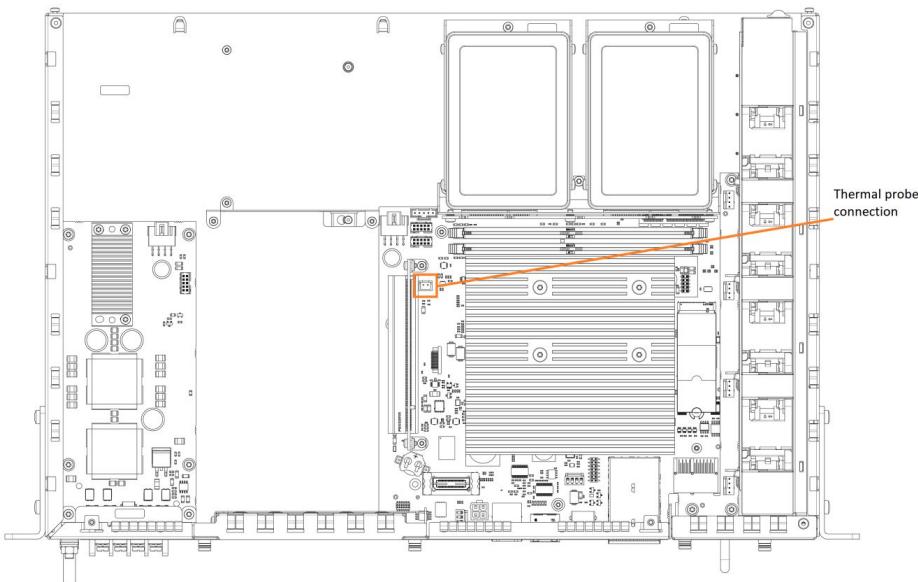
## Connecting the PCIe add-in card

## PRELIMINARY

Step_1	<p>Disconnect the PCIe riser by removing the 2 screws with a T8 Torx screwdriver.</p>	
Step_2	<p>Install the PCIe add-in card onto the PCIe riser. Mount the front plate adapter onto the PCIe add-in card's L-bracket. Fasten the front plate adapter screw to the L-bracket using a T10 Torx screwdriver (6 lbf·in torque).</p>	
Step_3	<p>Remove the 2 mounting screws from the rear mounting bracket using a T8 Torx screwdriver. Carefully insert the PCIe add-in card assembly into the unit by fastening the following 6 screws:</p> <ul style="list-style-type: none"> <li>• 2 T8 Torx screws for the riser card onto the server motherboard (4 lbf·in torque)</li> <li>• 2 T8 Torx screws for the PCIe add-in card into the rear mounting bracket (4 lbf·in torque)</li> <li>• 2 T10 Torx captive screws into the front plate (6 lbf·in torque)</li> </ul>	 

Installing a thermal probe for the PCIe add-in card

### Locating the thermal probe connection



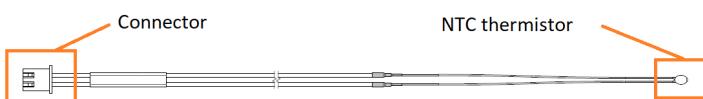
## Installing the thermal probe

Relevant sections:

[Managing customer added sensors](#)

[Platform cooling and thermal management](#)

[Monitoring sensors](#)



Step_1	Install the thermal probe in the connector as prescribed in the thermal probe specifications.
Step_2	<p>Affix the NTC thermistor to the PCIe card.</p> <p>Typically, thermistors are installed between the fins of the PCIe card heatsink. Do not forget to use glue that can withstand the temperature.</p> <p><b>NOTE:</b> Configuration will be performed once the platform is operational (thresholds, specific software configurations, etc.).</p>

## Closing the enclosure

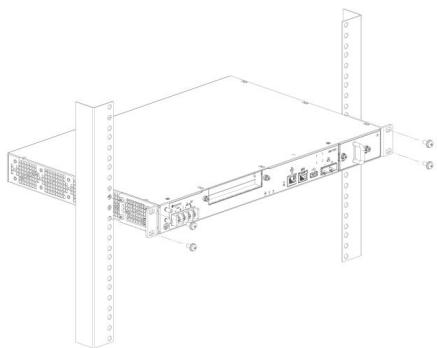
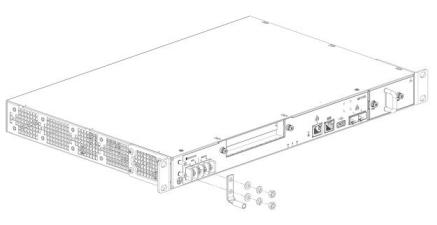
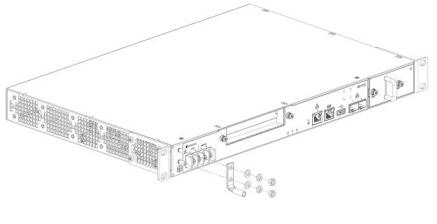
## PRELIMINARY

Step_1	Align the cover lock mechanisms with the cutouts on the chassis and slide it toward the front to fasten it into place.	
Step_2	Insert the 4 T8 Torx screws in the back and the 2 T8 Torx screws on top without turning them, making sure the holes on the cover and the holes on the chassis are properly aligned. <b>NOTE:</b> Tightening screws into unaligned holes will damage the threads.	
Step_3	Tighten the 6 screws using a T8 Torx screwdriver to lock the cover in place.	

## Racking the platform

The airflow of the platform goes from right to left, facing front. Ensure there is no physical obstruction that would hinder proper airflow when choosing a location for the platform in the rack.

## PRELIMINARY

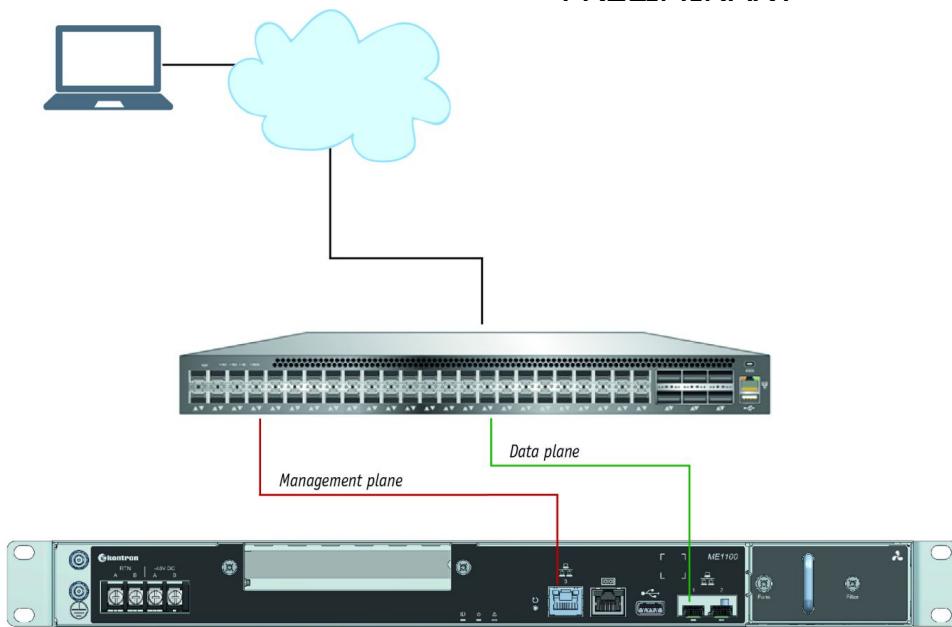
Step_1	Choose a location for the platform in the rack.	
Step_2	Insert the platform in the rack.	
Step_3	Fasten the platform to the rack using the appropriate fasteners.	
Step_4	If a ground lug is installed, remove the 2 nuts and washers from the ground lug studs. Take out the ground lug.	
Step_5	Strip 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. <b>NOTE:</b> The thread of the two chassis ground lugs is M5x0.8.	

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

## Connecting the network cables

Connect the network cables according to the image below:

1. Connect one RJ45 cable to port 3 for the management plane.
2. Connect one SFP or SFP+ cable to port 1 for the data plane.



CP0285

## Building and connecting the DC power cables



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

### 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.

Kontron suggests the following wire gauges for -48V DC and RTN: 14 AWG or 12 AWG.

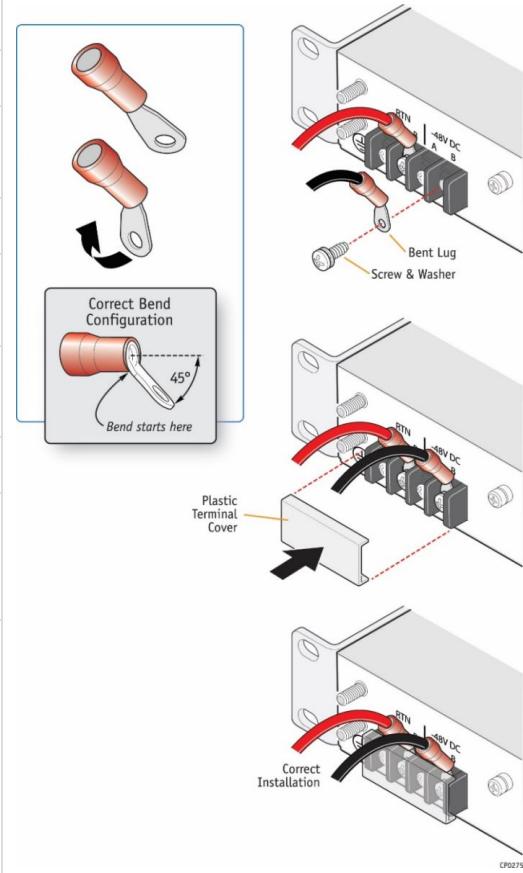
## PRELIMINARY

Description	Quantity	Manufacturer P/N	Link
Crimp lugs: <ul style="list-style-type: none"> <li>Molex insulated spade crimp lugs for 14-16 wire gauge</li> <li>Panduit insulated ring crimp lugs for 10-12 wire gauge</li> </ul>	2 (or 4 for redundancy)	19131-0023 or equivalent	<ul style="list-style-type: none"> <li><a href="#">Molex product catalog</a></li> <li><a href="#">Part details</a></li> </ul>
		EV10-6RB-Q or equivalent	<ul style="list-style-type: none"> <li><a href="#">Panduit product catalog</a></li> <li><a href="#">Part drawing</a></li> </ul>
Black stranded wire to build the power cable based on the length required: <ul style="list-style-type: none"> <li>14 AWG insulation diameter max.: 4.40 mm [ 0.175 in] for Molex crimp lugs</li> <li>12 AWG insulation diameter max.: 5.8 mm [0.23 in] for Panduit crimp lugs</li> </ul>	Length required		
Red stranded wire to build the power cable based on the length required: <ul style="list-style-type: none"> <li>14 AWG insulation diameter max.: 4.40 mm [ 0.175 in] for Molex crimp lug</li> <li>12 AWG insulation diameter max.: 5.8 mm [0.23 in] for Panduit crimp lug</li> </ul>	Length required		
Hand crimp tool: <ul style="list-style-type: none"> <li>Molex Premium Grade Hand Crimp Tool</li> <li>Panduit Hand Crimp Tool</li> </ul>	1	640010100 or equivalent	<ul style="list-style-type: none"> <li><a href="#">Molex product catalog</a></li> <li><a href="#">Application tooling specification sheet</a></li> </ul>
		CT-460 or equivalent	<ul style="list-style-type: none"> <li><a href="#">Panduit product catalog</a></li> <li><a href="#">Application tooling specification sheet</a></li> </ul>

### Procedure

## PRELIMINARY

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	Put the plastic terminal cover back in place once all the cables are screwed in place. <b>NOTE:</b> The power supply is reverse polarity protected. The unit will power on as soon as external power is applied (green power LED).



<span style="color: orange; font-size: 2em;">►</span> <p>If the ambient temperature is <b>below 10°C</b> and no sensor has exceeded its temperature thresholds, the fans will be on standby (not running and making no sound). Above that <b>10°C boundary</b>, the fans will spin at 8% of their maximum capacity. Refer to <a href="#">Platform cooling and thermal management</a> for more information about fan behavior over the entire operating temperature range.</p>
---

> You are now ready to start platform configuration.

## Confirming network links are established

Once the ME1100 power LED is **green ON** (normal blink or ON), confirm LAN connection with the management plane and data plane:

- The right LED on Port 3 (management) should be **green ON**
- The LED on SFP or SFP+ Port 1 should be **green ON**

Refer to [Platform components](#) for more information about LED location and behavior.

If LED behavior is not as expected, refer to your IT personnel to review upstream network status (the top-of-rack switch port might be disabled).

## Discovering or configuring the platform management IP

# PRELIMINARY

## address

The platform management IP address is the minimum required to access the Web UI, the monitoring interface and the KVM to install an operating system.

The IP address can be discovered or configured using the BIOS menu. When no OS is installed and the IP address is not known, the BIOS must be accessed via a serial console (physical connection).

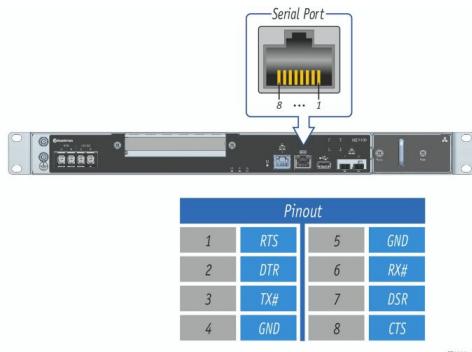
For detailed information on MAC addresses and IPs, refer to [Baseboard management controller - BMC](#) and [MAC addresses](#).

### Accessing the BIOS using a serial console (physical connection)

#### Prerequisites

1	A physical connection to the device is required. <b>NOTE:</b> The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the external computer. <ul style="list-style-type: none"><li>• Speed (Baud): 115200</li><li>• Data bits: 8</li><li>• Stop bits: 1</li><li>• Parity: None</li><li>• Flow Control: None</li><li>• Recommended emulation mode: VT100+</li></ul> <b>NOTE:</b> PuTTY is recommended.

#### Port location



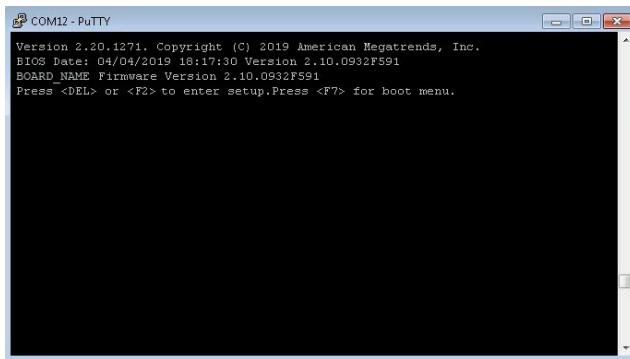
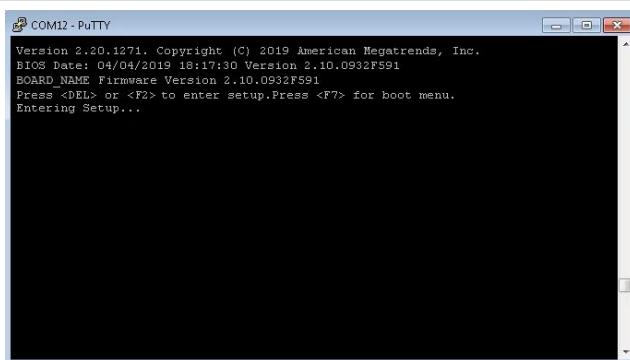
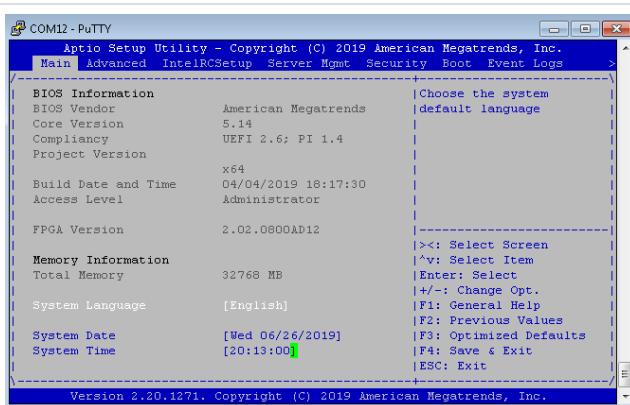
#### Access procedure

Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.
Step_2	Perform a server reset ( <b>Ctrl-break</b> hot key). <b>NOTE:</b> If an operating system is installed on the device, the hot key might not work properly. If this is the case, reset the server as recommended for the operating system. <b>NOTE:</b> When a server reset command is sent, it may take a few seconds for the BIOS sign on screen to display.

The screenshot shows a PuTTY terminal window titled 'COM12 - PuTTY'. The window displays a series of log messages from the BIOS initialization process. The text is in green and black, typical of a terminal log. The messages include:

```
COM12 - PuTTY
System Information
BOARD NAME BIOS Version: 2.10.0932F591 Date: "04/04/2019"
Intel RC Version: 02.05.00
CPU Info: Intel(R) Xeon(R) CPU D-1548 @ 2.00GHz
Memory Info: Memory Size: 32GB Memory Speed: 2400MHz RAS Mode: Indep
0x32 : CPU POST-Memory Initialization
0x4F : DXE IPL Start
0x68 : PCI HB Initialization.
0x70 : SB DXE Initialization.
0x79 : CSM Driver Entry point
0x91 : Connecting Drivers.
0x92 : PCI Bus Initialization.
0x94 : PCI Bus Enumeration.
0x95 : PCI Bus Request Resources.
0x96 : PCI Bus Assign Resources.
0x91 : Connecting Drivers.
0x92 : PCI Bus Initialization.
0x97 : Console Output devices connect.
```

## PRELIMINARY

		
Step_3	<p>When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.</p> <p><b>NOTE:</b> It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup...".</p>	
Step_4	<p>The BIOS sign on screen displays "Entering Setup...".</p> <p><b>NOTE:</b> It will take several seconds to display and enter the BIOS setup menu.</p>	
Step_5	The BIOS setup menu is displayed.	

### Accessing the BMC network configuration menu

# PRELIMINARY

Step_1	<p>From the BIOS menu, use the arrow keys to select <b>Server Mgmt</b>.</p>	<pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IntelRCSsetup [Server Mgmt] Security Boot Event Logs  BIOS Information BIOS Vendor American Megatrends  Choose the system Core Version 5.14  default language Compliance UEFI 2.6; PI 1.4 Project Version  Build Date and Time 06/26/2019 09:12:28 Access Level Administrator  FPGA Version 2.02.0800AD12  Memory Information Total Memory 32768 MB  System Language [English] System Date [Wed 07/10/2019] System Time [13:47:54]   &gt;&lt;: Select Screen  ^v: Select Item  Enter: Select  +/-: Change Opt.  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Exit  ESC: Exit  Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. AB </pre>
Step_2	<p>Use the arrow keys to select <b>BMC network configuration</b>.</p>	<pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IntelRCSsetup [Server Mgmt] Security Boot Event Logs  BMC Interface(s) KCS, USB Wait For BMC [Disabled] FRB-2 Timer [Enabled] FRB-2 Timer timeout [6 minutes] FRB-2 Timer Policy [Power Cycle]  OS Watchdog Timer [Disabled] OS Wtd Timer Timeout [10 minutes] OS Wtd Timer Policy [Reset] Serial Mux [Disabled]   &gt; System Event Log  &gt; View FRU information  &gt; BMC network configuration  &gt; View System Event Log  &gt; BMC User Settings  &gt; BMC Warm Reset   &gt;&lt;: Select Screen  ^v: Select Item  Enter: Select  +/-: Change Opt.  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Exit  ESC: Exit  Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. AB </pre>
Step_3	<p>The <b>BMC network configuration</b> menu is displayed.</p> <p><b>NOTE:</b> When the platform is powered up after being shut off, the BIOS may load before the BMC has received its IP address. In this case, the BIOS menu information will need to be refreshed by restarting the server and re-entering the BIOS.</p>	<pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. [Server Mgmt]  --BMC network configuration-- ***** Configure IPV4 support *****  Lan channel 1 Configuration Address [Unspecified] source Current Configuration DynamicAddressBmcDhcp Address source Station IP address 172.16.205.245 Subnet mask 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 172.16.0.1 Router MAC address 00-05-64-2F-10-5F  Lan channel 2   &gt;&lt;: Select Screen  ^v: Select Item  Enter: Select  +/-: Change Opt.  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Exit  ESC: Exit  Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. AB </pre>

From the BMC network configuration menu, you have two options according to your network scheme:

- To discover the DHCP IP address, go to section [DHCP](#)
- To configure a static IP address, go to section [static](#)

In this use case, only BMC LAN channel 1 will be configured as the management plane is connected through port 3. Refer to [Product architecture](#) for a visual representation and information on network connectivity.

## Discovering the DHCP management IP address

# PRELIMINARY

Step_1	<p>From the BMC network configuration menu.</p> <p>If an IP address is displayed, make a note of it as it is your management IP address ( BMC MNGMT_IP ).</p> <p><b>OR</b></p> <p>If the IP address displayed is 0.0.0.0, perform optional steps 2, 3 and 4.</p> <p><b>NOTE:</b> When the platform is powered up after being shut off, the BIOS may load before the BMC has received its IP address via DHCP. In this case, the BIOS menu information will need to be refreshed (steps 2 to 4).</p>	<p>The screenshot shows the 'Server Mgmt' menu of the Aptio Setup Utility. Under 'BMC network configuration', it lists 'Configure IPv4 support' and 'Lan channel 1'. Lan channel 1 details include 'Configuration Address [Unspecified]', 'Current Configuration DynamicAddressBmcDhcp', and 'Address source'. Below this, 'Station IP address' is 172.16.205.245, 'Subnet mask' is 255.255.0.0, 'Station MAC address' is 00-A0-A5-D6-33-2A, 'Router IP address' is 172.16.0.1, and 'Router MAC address' is 00-05-64-2F-10-5F. A key mapping legend at the top right describes keys like F1, F2, F3, F4, Esc, and arrow keys for various functions like Select, Enter, and Change Opt.</p>
Step_2	(Optional) Navigate to Save & Exit.	<p>The screenshot shows the 'Save &amp; Exit' menu of the Aptio Setup Utility. It includes options like 'Save Changes and Reset', 'Discard Changes and Reset', 'Save Changes', 'Discard Changes', 'Default Options', 'Restore Defaults', 'Save as User Defaults', 'Restore User Defaults', 'Boot Override', 'AMIFWUpdate', and 'AMI Virtual CDROM0 1.00'. A key mapping legend at the bottom right describes keys like F1, F2, F3, F4, Esc, and arrow keys for various functions like Select, Enter, and Change Opt.</p>
Step_3	(Optional) Select Save Changes and Exit or Discard Changes and Exit , this will perform a server reset.	<p>The screenshot shows the 'Save &amp; Exit' menu with a confirmation dialog box titled 'Save &amp; Exit Setup' asking 'Save configuration and exit?'. The 'Yes' button is highlighted. The background menu includes options like 'Save Options', 'Save Changes and Exit', 'Discard Changes and Exit', 'Save Changes and Reset', 'Discard Changes and R...', 'Save Changes', 'Discard Changes', 'Default Options', 'Restore Defaults', 'Save as User Defaults', 'Restore User Defaults', 'Boot Override', 'AMIFWUpdate', and 'AMI Virtual CDROM0 1.00'. A key mapping legend at the bottom right describes keys like F1, F2, F3, F4, Esc, and arrow keys for various functions like Select, Enter, and Change Opt.</p>
Step_4	(Optional) When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu. Then, access the Server Mgmt menu and select BMC network configuration . Make a note of the address displayed as it is your management IP address ( BMC MNGMT_IP ).	

## Configuring a static management IP address

**NOTE:** If you are in a DHCP network, skip this section.

## PRELIMINARY

Step_1	<p>From the BMC network configuration menu, select the Configuration Address source option for the LAN interface to configure (LAN channel 1 in this example).</p>	<pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Server Mgmt  /-----BMC network configuration----- *****Configure IPv4 support***** *****Lan channel 1***** Configuration Address source [Unspecified] Current Configuration DynamicAddressBmcDhcp Address source Station IP address 172.16.205.245 Subnet mask 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 172.16.0.1 Router MAC address 00-05-64-2F-10-5F *****Lan channel 2***** Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. </pre>
Step_2	Select Static.	<pre> /---- Configuration Address source ---\   Unspecified   <b>Static</b>   DynamicBmcDhcp   DynamicBmcNonDhcp \-----/ </pre>
Step_3	<p>Change the Station IP address . NOTE: This is the management IP address ( BMC MNGMT_IP ).</p>	<pre> Lan channel 1 Configuration Address source [Static] Station IP address 172.16.205.245 Subnet mask 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00-00 </pre>
Step_4	Change the Subnet mask .	<pre> Lan channel 1 Configuration Address source [Static] Station IP address 172.16.205.245 Subnet mask 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00-00 </pre>
Step_5	(Optional) Change the Router IP address .	<pre> Lan channel 1 Configuration Address source [Static] Station IP address 172.16.205.245 Subnet mask 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 172.16.0.1 Router MAC address 00-00-00-00-00-00 </pre>
Step_6	Confirm the configuration has changed and exit BMC network configuration using the ESC key.	<pre> Lan channel 1 Configuration Address source [Static] Station IP address 172.16.205.245 Subnet mask 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 172.16.0.1 Router MAC address 00-05-64-2F-10-5F </pre>

> With your management IP (BMC MNGMT\_IP), 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 (CentOS 7.4 or latest version is recommended).
Step_2	Confirm the OS version to be installed includes or is compatible with the following network interface drivers: igb and ixgbe .
Step_3	If applicable, download the ISO file of the OS to be installed.

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

For information on components, refer to the [PCI mapping](#).

## Installing an operating system

# PRELIMINARY

## Prerequisites

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

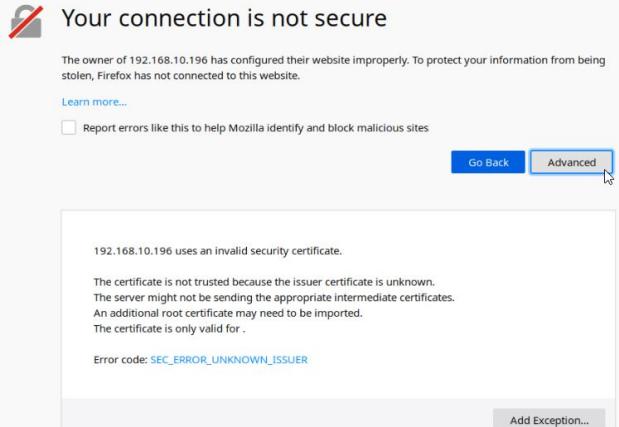
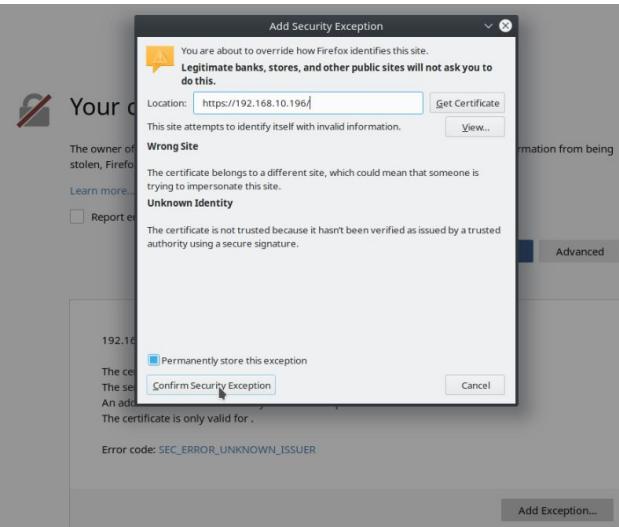
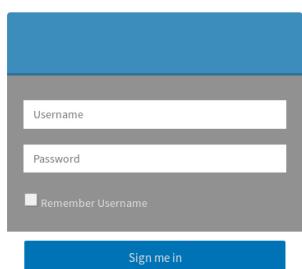
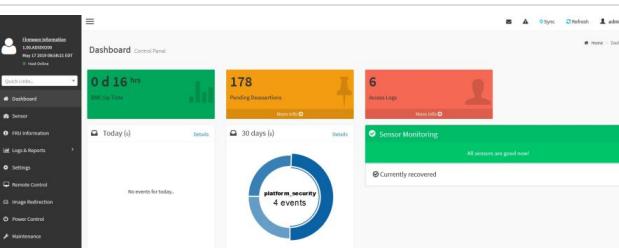
## Browser considerations

<b>HTML5</b>	To connect to the Web UI, a Web browser supporting HTML5 is required.
<b>HTTPS self-signed certificate</b>	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.
<b>File download permission</b>	File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser's documentation.
<b>Cookies</b>	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

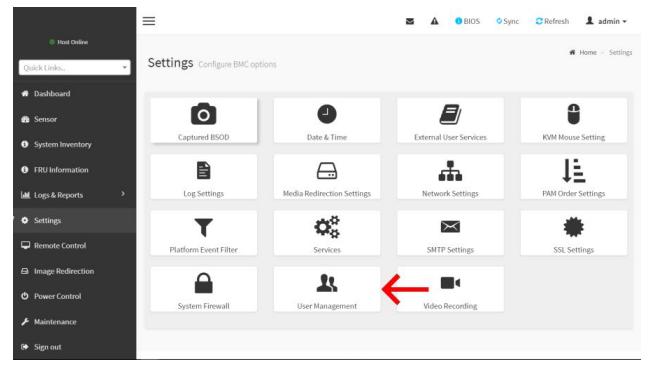
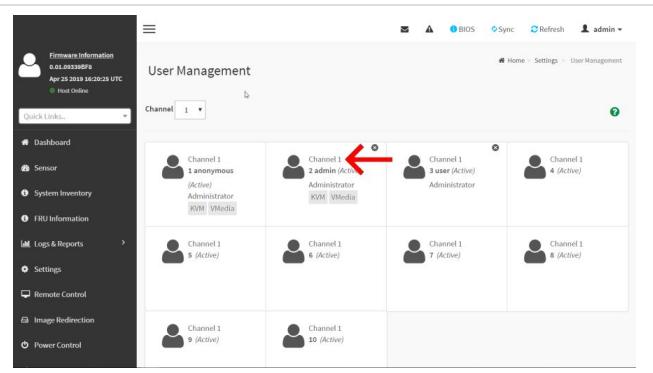
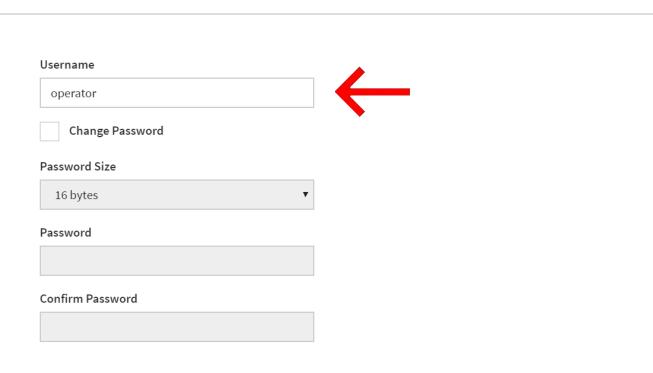
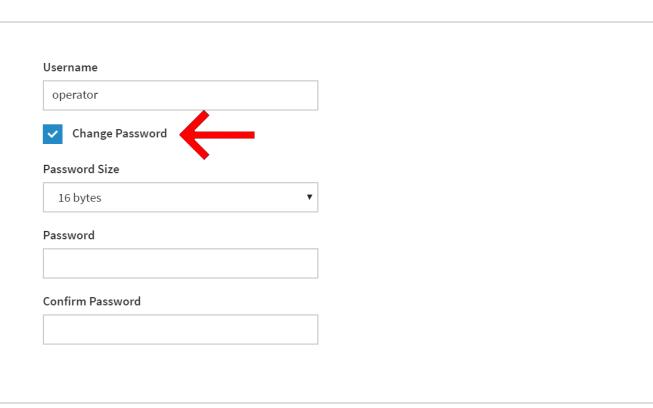
# PRELIMINARY

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

# PRELIMINARY

## Changing the user name and password

**NOTE:** All user names and passwords must have a minimum of 8 characters .

Step_1	<p>Click on <b>Settings</b> in the left side menu and click on <b>User Management</b> .</p> 
Step_2	<p>Select the user to manage.</p> <p><b>NOTE:</b> The first and second users are reserved fields, therefore, their usernames can't be modified.</p> 
Step_3	<p>Change field <b>Username</b> if required.</p> 
Step_4	<p>Check the <b>Change Password</b> box.</p> 
Step_5	<p>Create a new password.</p> 

## PRELIMINARY

Step\_6 Confirm the password.

Username  
operator

Change Password

Password Size  
16 bytes

Password  
.....

Confirm Password  
..... ←

Step\_7 Press **Save**.

Email Format  
AMI-Format

Email ID

Existing SSH Key  
Not Available

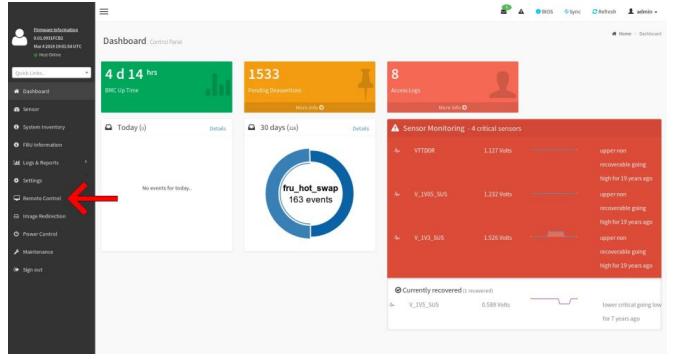
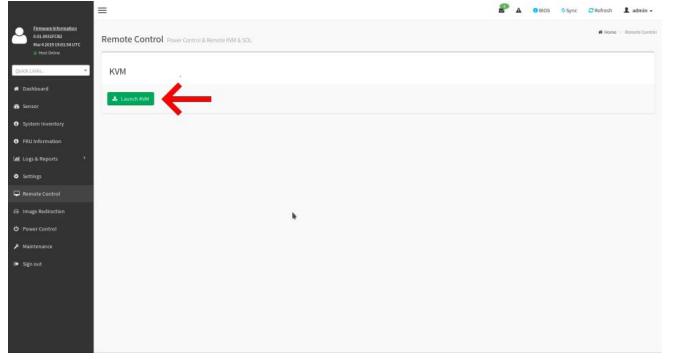
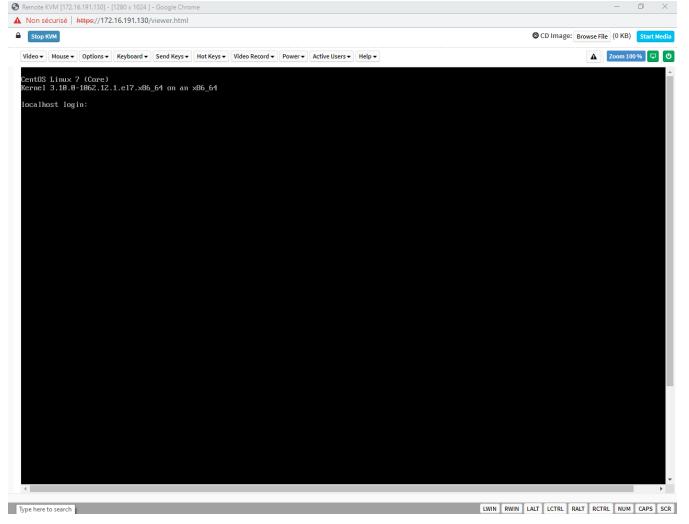
Upload SSH Key  
 →

Delete Save →

### Launching the KVM

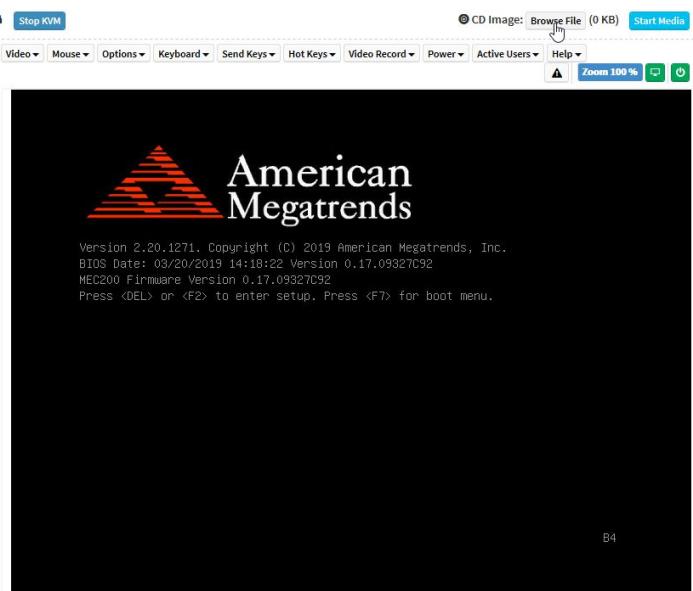
The Web UI allows remote control of the server through a KVM (Keyboard, Video, Mouse) interface.

# PRELIMINARY

<p><b>Step_1</b> From the left menu, click on <b>Remote Control</b>.</p> 	<p><b>Step_2</b> From the <b>Remote Control</b> menu, click on the <b>Launch KVM</b> button.</p> 
<p><b>Step_3</b> A new browser window opens and displays the server screen.  <b>NOTE:</b> If an OS is installed, the image displayed might be that of the OS.</p> 	

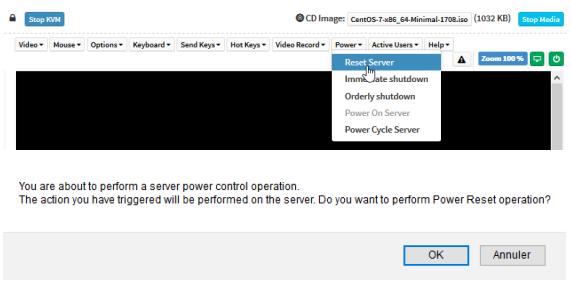
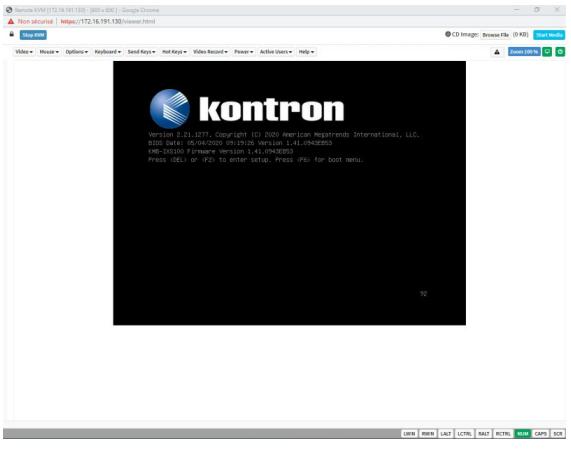
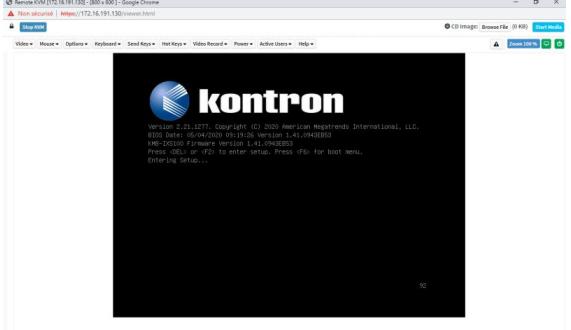
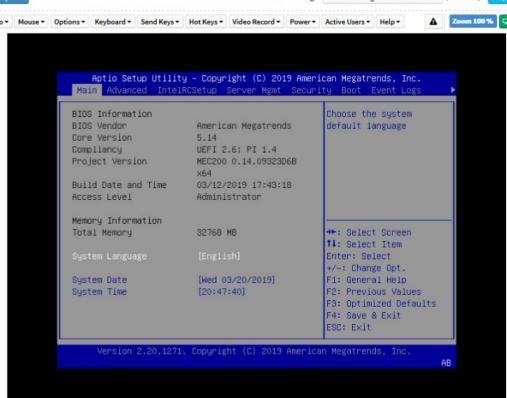
Mounting the operating system image via virtual media

## PRELIMINARY

Step_1	<p>From the KVM view of the server screen, click on <b>Browse File</b> at the top right of the screen. Select the ISO file to be mounted and click on <b>Open</b>.</p>	 <p>The screenshot shows the KVM interface with the American Megatrends logo at the top. Below it, the BIOS version is listed: Version 2.20.1271, Copyright (C) 2019 American Megatrends, Inc. BIOS Date: 03/20/2019 14:18:22 Version 0.17.09327C92 MEC200 Firmware Version 0.17.09327C92. A note says Press &lt;DEL&gt; or &lt;F2&gt; to enter setup. Press &lt;F7&gt; for boot menu.</p>
Step_2	<p>Once the ISO file is loaded, click on <b>Start Media</b> at the top right of the screen. <b>NOTE:</b> Once clicked, the Start Media button becomes the <b>Stop Media</b> button.</p>	 <p>The first screenshot shows the KVM interface with the 'Start Media' button highlighted. The second screenshot shows the same interface after the button has been clicked, now labeled 'Stop Media'.</p>

### Accessing the BIOS setup menu

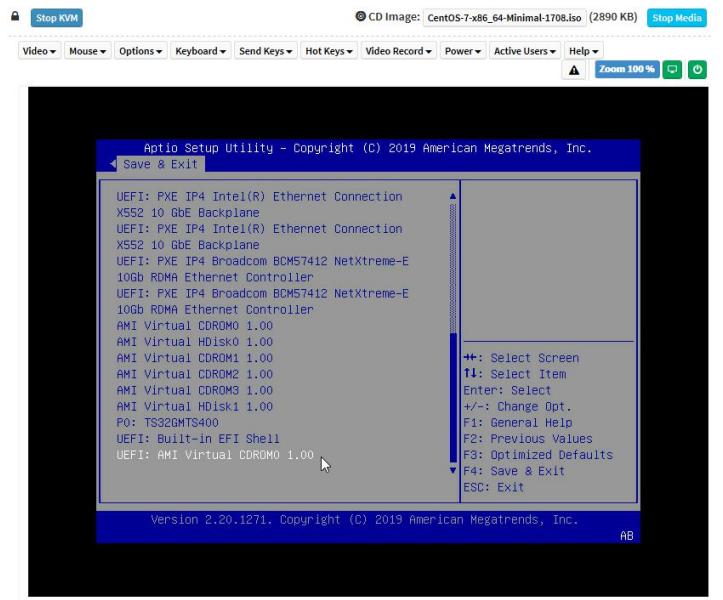
# PRELIMINARY

Step_1	<p>From the <b>Power</b> drop-down menu, select <b>Reset Server</b> to access the BIOS menu. Click on <b>OK</b> to confirm the operation.</p> <p><b>NOTE:</b> When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.</p>	
Step_2	<p>When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.</p> <p><b>NOTE:</b> It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup..."</p> <p><b>Tip:</b> Some users are pressing DEL/F2 many times and very rapidly, to make sure the server catches the key and enters the BIOS setup menu. Doing this may lead to following message on the KVM display: <b>HID Queue is about to get full. Kindly hold on a second(s)..</b> Kontron suggests modifying the <b>Setup Prompt Timeout</b> parameter to give users more time to react. Keeping the focus (single-tasking) on the KVM window is also a good practice to enter the BIOS setup menu each time it is needed.</p> <p>Parameter <b>Setup Prompt Timeout</b> is found in the <b>Boot</b> tab of the BIOS setup menu. The default value is 1 second, but changing it to a value between 3 and 10 seconds is a good target range.</p>	
Step_3	<p>The BIOS sign on screen displays "Entering Setup...".</p> <p><b>NOTE:</b> It will take several seconds to display and enter the BIOS setup menu.</p>	
Step_4	<p>The BIOS setup menu will be displayed.</p>	

# PRELIMINARY

## Selecting the boot order from boot override

Step\_1 From the BIOS setup menu and using the keyboard arrows, select the **Save & Exit** menu. In the **Boot Override** section, select **UEFI: AMI Virtual CDROM0 1.00** and press **Enter**. The server will reboot and the media installation process will start.



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

## Completing operating system installation

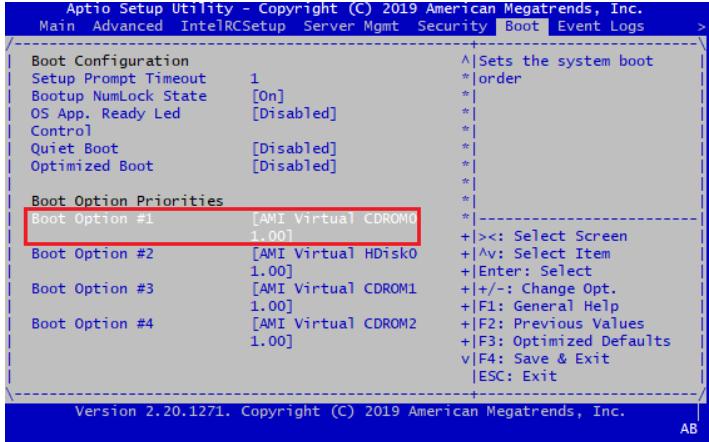
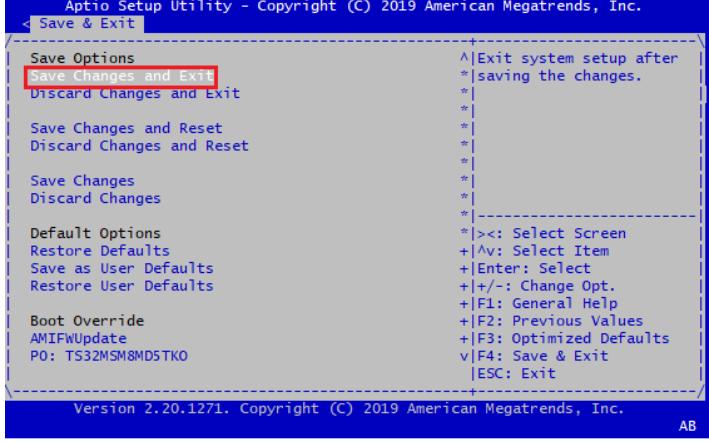
Step\_1 Complete the installation by following the on-screen prompts of the specific OS installed.

## (Optional) Changing the boot order in the BIOS menu



After installation, if booting from network (PXE) occurs and is not desired, your operating system installer may not have modified the BIOS boot order. To correct this, enter BIOS setup again and follow the steps below.

## PRELIMINARY

Step_1	<p>From the BIOS setup menu, use the keyboard arrows to select the Boot menu. Configure the boot order as desired.</p>	 <pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IntelRCSetup Server Mgmt Security Boot Event Logs  Boot Configuration Setup Prompt Timeout 1 Bootup NumLock State [On] OS App. Ready Led [Disabled] Control Quiet Boot [Disabled] Optimized Boot [Disabled]  Boot Option Priorities Boot Option #1 [AMI Virtual CDROM 1.00] Boot Option #2 [AMI Virtual HDisk0 1.00] Boot Option #3 [AMI Virtual CDROM1 1.00] Boot Option #4 [AMI Virtual CDROM2 1.00]  Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. AB </pre>
Step_2	<p>Using the keyboard arrows, select the Save &amp; Exit menu, go to Save Changes and Exit and press Enter to confirm and save the new boot order.</p>	 <pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Save &amp; Exit  Save Options Save Changes and Exit Discard Changes and Exit  Save Changes and Reset Discard Changes and Reset  Save Changes Discard Changes  Default Options Restore Defaults Save as User Defaults Restore User Defaults  Boot Override AMIFWUpdate PO: TS32MSM8MD5TKO  Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. AB </pre>

## Verifying operating system installation

	<p>All the results and commands may vary depending on the operating system and the devices added.</p>
---	---

Step_1	<p>Reboot the OS as recommended, then access the OS command prompt.</p>
Step_2	<p>Verify that no error messages or warnings are displayed in <code>dmesg</code> using the following commands.</p> <pre>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"</pre> <p><b>NOTE:</b> If there are any messages or warnings displayed, refer to the operating system's documentation to fix them.</p>
Step_3	<p>Verify that the DIMMs are detected.</p> <pre>LocalServer_OSPrompt:~# free -h</pre>
Step_4	<p>Verify that all the storage devices are detected.</p> <pre>LocalServer_OSPrompt:~# lsblk</pre>
Step_5	<p>Confirm the control plane network interface controller is loaded by the <code>igb</code> driver.</p> <pre>LocalServer_OSPrompt:~# dmesg   grep igb</pre>

## PRELIMINARY

**NOTE:** You should discover one 1GbE NIC.

```
[ 5.127127] igb 0000:09:00.0 eth0: (PCIe 2.1 x8) 3.0W Gen X4 50.00MHz 50.00Hz
[ 5.237322] igb 0000:09:00.0: eth0: PBA No: 000001-000
[ 5.237323] igb 0000:09:00.0: Using MSI-X interrupts, 4 rx queue(s), 4 tx queue(s)
[ 18.287293] igb 0000:09:00.0 eno3: igb: eno3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
```

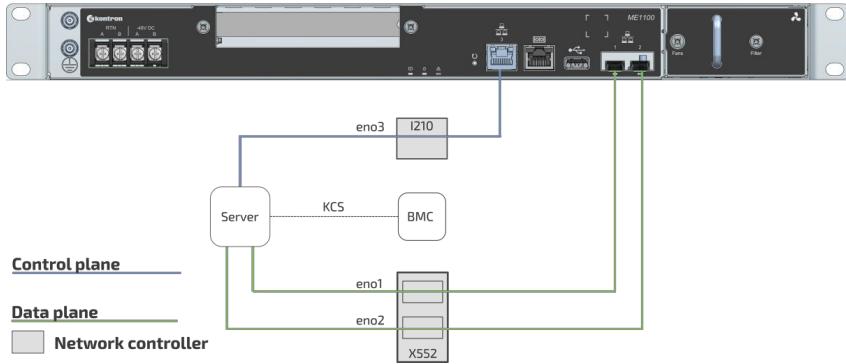
- Step\_6** Confirm the data plane network interface controllers are loaded by the **ixgbe** driver.  
**LocalServer\_OSPrompt:**~# **dmesg | grep ixgbe**  
**NOTE:** You should discover two 10GbE NIC.

```
[ 6.516596] ixgbe 0000:04:00.1: MAC: 5, PHY: 14, SFP+: 3, PBA No: 000200-000
[ 6.523639] ixgbe 0000:04:00.1: 00:a0:a5:d6:33:2e
[ 6.674120] ixgbe 0000:04:00.1: Intel(R) 10 Gigabit Network Connection
[ 13.433172] ixgbe 0000:04:00.0: registered PHC device on eno1
[ 19.225229] ixgbe 0000:04:00.1: registered PHC device on eno2
[ 19.319333] ixgbe 0000:04:00.1 eno2: detected SFP+: 3
[ 19.967523] ixgbe 0000:04:00.1 eno2: NIC Link is Up 10 Gbps, Flow Control: RX/TX
```

- Step\_7** Confirm that all the network interfaces are detected.  
**LocalServer\_OSPrompt:**~# **ip address**  
**NOTE:** You should discover one 1GbE NIC and two 10GbE NIC.

```
[root@localhost ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 brd :: scope host
            valid_lft forever preferred_lft forever
2: eno3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:a0:a5:d6:33:2c brd ff:ff:ff:ff:ff:ff
        inet 172.16.206.11/16 brd 172.16.255.255 scope global noprefixroute dynamic eno3
            valid_lft 1208786sec preferred_lft 1208786sec
        inet6 fe80::d2ae:4046%eno3/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:a0:a5:d6:33:2d brd ff:ff:ff:ff:ff:ff
4: eno2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:a0:a5:d6:33:2e brd ff:ff:ff:ff:ff:ff
        inet6 fe80::2a0:a5ff:fed6:332e/64 scope link
            valid_lft forever preferred_lft forever
5: eno2.4093@eno2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:a0:a5:d6:33:2e brd ff:ff:ff:ff:ff:ff
        inet6 fe80::2a0:a5ff:fed6:332e/64 scope link
            valid_lft forever preferred_lft forever
```

- Step\_8** Configure network interface controllers based on your requirements.  
**NOTE:** Interface names may change depending on the OS installed. However, parameters Bus:Device.Function stay the same for the interface regardless of the operating system.



- Step\_9** Install **ipmitool** and **pciutils** using the package manager, and update the operating system packages. The **ipmitool** version recommended is 1.8.18.  
**Example:**  
**LocalServer\_OSPrompt:**~# **yum update**  
**LocalServer\_OSPrompt:**~# **yum install ipmitool**  
**LocalServer\_OSPrompt:**~# **yum install pciutils**

**NOTE:** Updating the packages may take a few minutes.

- Step\_10** (Optional) If a PCIe add-in card is installed, verify that the card is detected.  
**LocalServer\_OSPrompt:**~# **lspci**

```
[root@localhost ~]# lspci
[ 00:00.0 Host bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DMII (rev 03)
[ 00:01.0 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 1 (rev 03)
[ 00:01.1 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 1 (rev 03)
[ 00:02.0 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 2 (rev 03)
[ 00:02.2 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 2 (rev 03)
[ 00:03.0 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 3 (rev 03)
[ 00:03.2 System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO HPC Plug (rev 03)
[ 00:05.0 System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO RAS/Control Status/Global Errors (rev 03)
[ 00:05.4 PIC: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D I/O APIC (rev 03)
[ 00:16.0 Communication controller: Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller #1 (rev 04)
[ 00:16.1 Communication controller: Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller #2 (rev 04)
[ 00:16.4 PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #1 (rev d5)
[ 00:1d.0 USB controller: Intel Corporation 8 Series/C220 Series Chipset Family USB EHCI #1 (rev 05)
[ 00:1d.1 SATA controller: Intel Corporation C224 Series Chipset Family Server Standard SKO IFC Controller (rev 05)
[ 00:1d.2 SATA controller: Intel Corporation 8 Series/C220 Series Chipset Family 6-port SATA Controller 1 [AHCI mode] (rev 05)
[ 00:1f.3 SMBus: Intel Corporation 8 Series/C220 Series Chipset Family SMBus Controller (rev 05)
```

- Step\_11** Verify communication between the operating system and the BMC.  
**LocalServer\_OSPrompt:**~# **ipmitool mc info**

```
LocalServer_OSPrompt:~# ipmitool mc info
Device ID          : 32
Device Revision    : 1
Firmware Revision  : 0.01
IPMI Version       : 2.0
Manufacturer ID    : 15000
Manufacturer Name   : Kontron
Product ID         : 1100 (0x044c)
Product Name        : Unknown (0x44C)
Device Available   : yes
Provides Device SDRs : no
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
```

## PRELIMINARY

```
FRU Inventory Device
IPMB Event Receiver
IPMB Event Generator
Chassis Device
Aux Firmware Rev Info
0x09
0x33
0x9b
0xf8
```

## Benchmarking an application

Install your application and proceed with benchmarking.

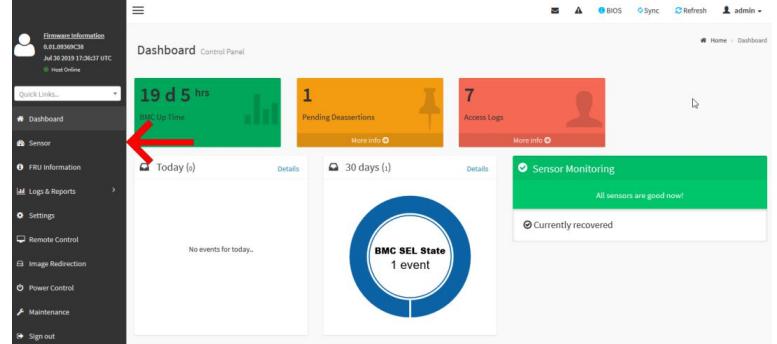
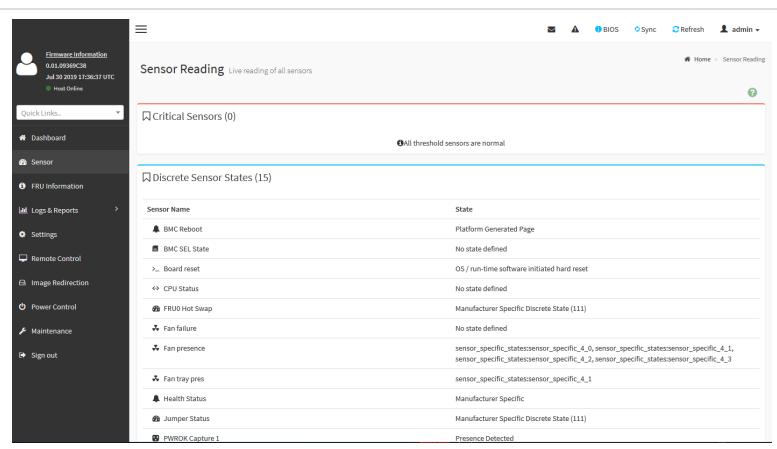
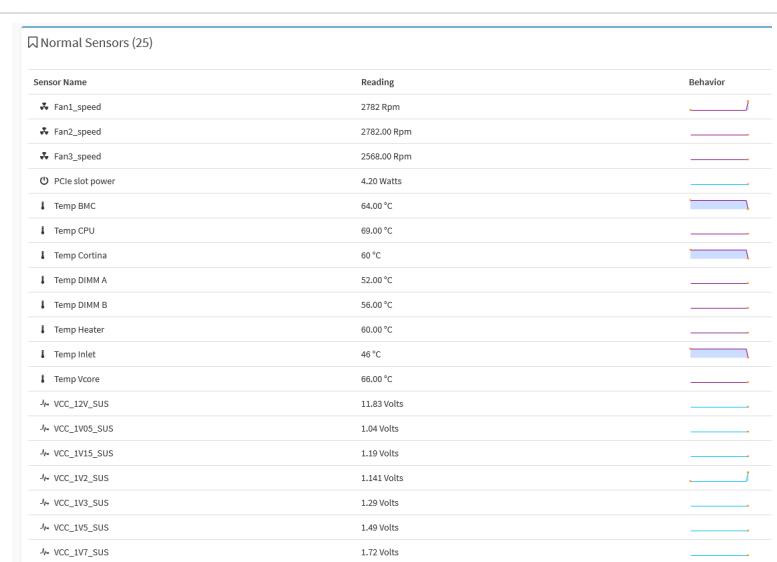
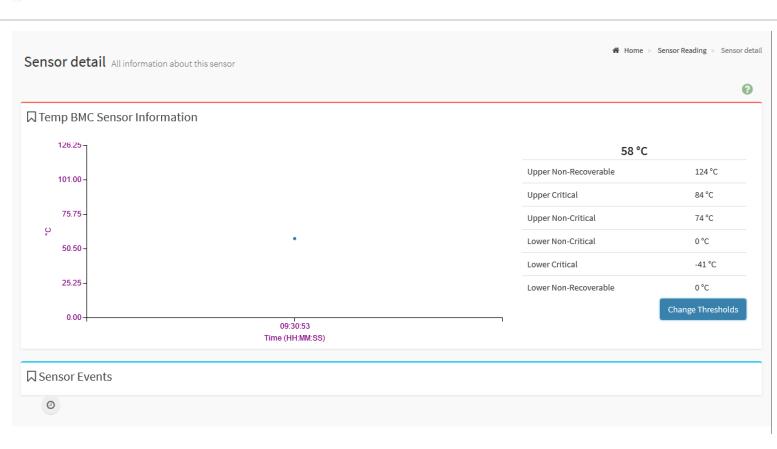
## Monitoring platform sensors using the Web UI

NOTE: Refer to [Accessing a BMC on an ME1100](#) to access the BMC Web UI.

The key sensors to look at are the following:

- Temperature sensors
- Power sensors

## PRELIMINARY

Step_1	Access the BMC Web UI.	
Step_2	From the left-side menu, click on Sensor .	
Step_3	The sensor list will be displayed.	
Step_4	Scroll down to see the list of sensors.	
Step_5	Click on a sensor to see more details.	

For a list of all the sensors, refer to [Sensor list](#).

For more monitoring methods refer to [Monitoring sensors](#).

## Managing PCIe add-in card temperature for system cooling

# PRELIMINARY

Relevant sections:

[Platform cooling and thermal management](#)

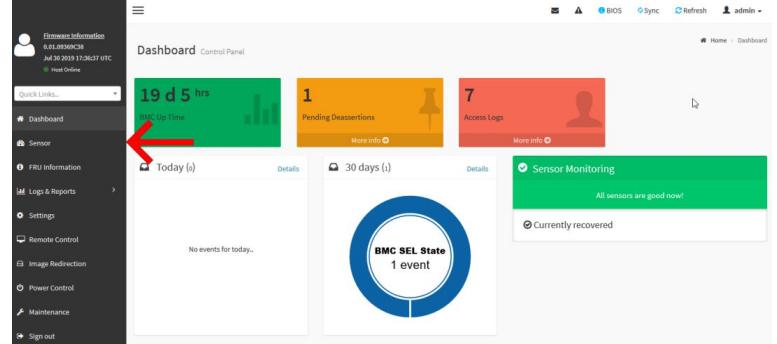
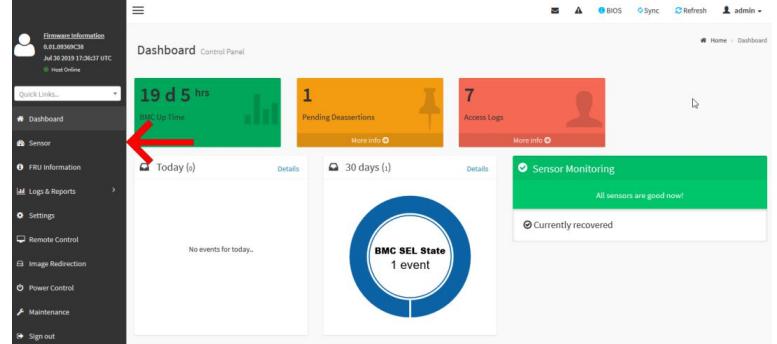
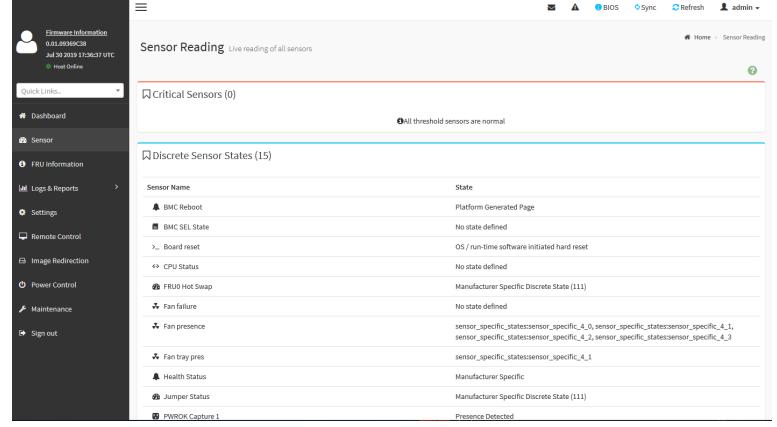
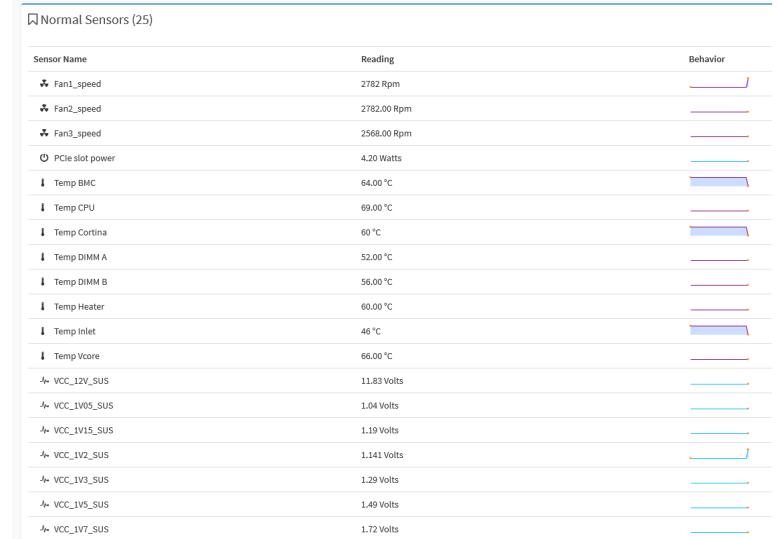
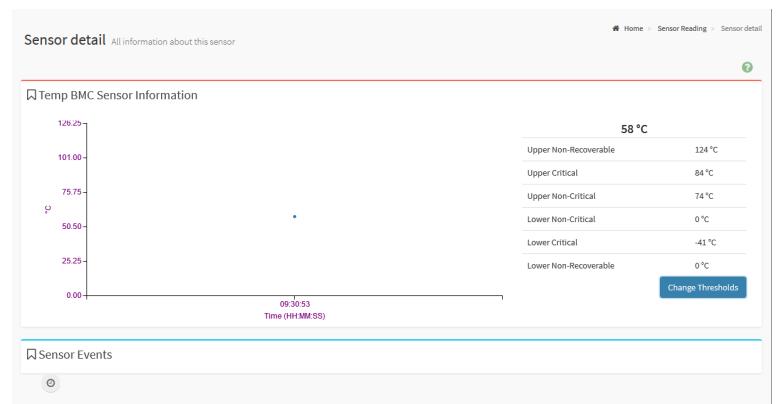
[Managing customer added sensors](#)

[Monitoring sensors](#)

## Accessing the Web UI

NOTE: Refer to [Accessing a BMC on an ME1100](#) to access the BMC Web UI.

# PRELIMINARY

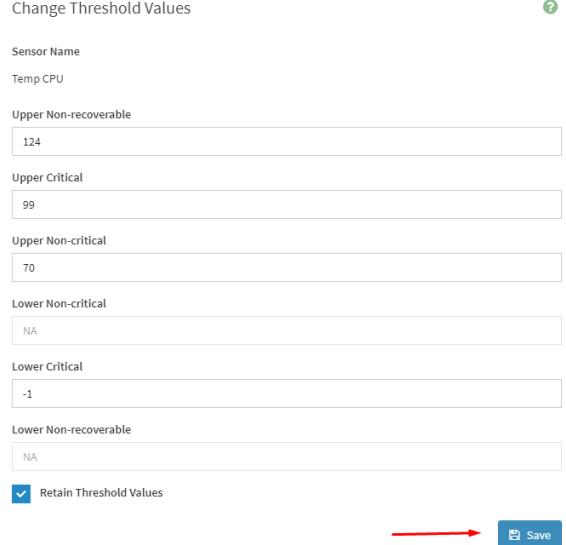
Step_1	Access the BMC Web UI.	
Step_2	From the left-side menu, click on Sensor .	
Step_3	The sensor list will be displayed.	
Step_4	Scroll down to see the list of sensors.	
Step_5	Click on a sensor to see more details.	

## Configuring the PCIe add-in card temperature sensor thresholds

The Temp NTC sensor is the one linked to the thermal probe physically connected in the platform. Its thresholds need to be set according to the specific parameters and uses of the PCIe add-in card installed. Proceed as shown below with the

# PRELIMINARY

appropriate sensor (Temp NTC).

Step_1	From the sensor detail page, click on <b>Change Thresholds</b> .	 <p>The screenshot shows a graph for the Temp PCIe sensor. The y-axis represents temperature in °C, with a red arrow pointing to the value 58 °C. The x-axis represents time in HH:MM:SS. Below the graph, a table lists the following threshold values:</p> <table border="1"> <thead> <tr> <th></th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Upper Non-Recoverable</td> <td>124 °C</td> </tr> <tr> <td>Upper Critical</td> <td>84 °C</td> </tr> <tr> <td>Upper Non-Critical</td> <td>74 °C</td> </tr> <tr> <td>Lower Non-Critical</td> <td>0 °C</td> </tr> <tr> <td>Lower Critical</td> <td>-41 °C</td> </tr> <tr> <td>Lower Non-recoverable</td> <td>-50 °C</td> </tr> </tbody> </table> <p>A blue button labeled "Change Thresholds" is located at the bottom right of the graph area.</p>		Value	Upper Non-Recoverable	124 °C	Upper Critical	84 °C	Upper Non-Critical	74 °C	Lower Non-Critical	0 °C	Lower Critical	-41 °C	Lower Non-recoverable	-50 °C
	Value															
Upper Non-Recoverable	124 °C															
Upper Critical	84 °C															
Upper Non-Critical	74 °C															
Lower Non-Critical	0 °C															
Lower Critical	-41 °C															
Lower Non-recoverable	-50 °C															
Step_2	<p>Set the thresholds as desired and click on <b>Save</b>.</p> <p>Optional: Check <b>Retain Thresholds</b> if you wish to keep the set thresholds after a BMC reboot</p>	 <p>The screenshot shows the "Change Threshold Values" configuration page for the Temp CPU sensor. It includes fields for setting various threshold levels and a checkbox for retaining them across reboots. A red arrow points to the "Save" button.</p> <p>Fields shown:</p> <ul style="list-style-type: none"> <li>Sensor Name: Temp CPU</li> <li>Upper Non-recoverable: 124</li> <li>Upper Critical: 99</li> <li>Upper Non-critical: 70</li> <li>Lower Non-critical: NA</li> <li>Lower Critical: -1</li> <li>Lower Non-recoverable: NA</li> <li><input checked="" type="checkbox"/> Retain Threshold Values</li> </ul> <p>A red arrow points to the "Save" button.</p>														

## Planning

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

Children

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

## Environmental considerations

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

The ME1100 platform has been designed to work over the extended temperature range of -40°C to +65°C (-40°F to +149°F) 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.

An ingress protection rating of IP55 has been achieved using the Harmony 2U Wall/Pole Mount Cabinet from SPC ([www.spc.net](http://www.spc.net) – Harmony Edge model 10705-030-004 Kontron 2RU Cabinet with Fan System). A complete test report is available to qualified customers upon request.

When powering up the ME1100 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 ME1100 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 ME1100 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 ME1100 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

*{This article provides power supply electrical specifications and explains how to estimate power consumption based on various use cases.}*

### DC power supply input voltage and current requirements

DC input voltage	
Nominal	-54 VDC
Minimum	-40 VDC
Maximum	-57 VDC
DC input current	
Maximum	6.45 A at -40 VDC; 4.52 A at -57 VDC
Power input	
Maximum	258 W

### AC power supply input voltage and current requirements

AC input voltage	
Nominal	115/230 VAC
Minimum	90 VAC
Maximum	265 VAC
DC input current	
Maximum	3.5 A at 90 VAC; 1.2A at 265 VAC
Power input	
Maximum	300 W

### Power consumption example

The power consumption of the following configuration is 142 W.

Measurements were taken at an ambient temperature of 25°C with the fans at their maximum speed while running a stress test application.

## PRELIMINARY

Components	Quantity	Notes
240 W DC PSU	1	
Fans	3	23 W per fan (at maximum speed)
45 W TDP CPU	1	
4 GB UDIMM	2	
SATA 32 GB M.2 SSD	1	
10 G Base-SR SFP+	2	
50 W PCIe add-in card	0	
2.5-in SATA SSD	0	

Various options will increase power consumption when compared to that of the example configuration:

Components	Quantity	Additional system power consumption from 142 W example configuration
65 W TDP CPU <i>instead of the 45 W TDP CPU</i>	1	22 W
32 GB RDIMM <i>Instead of the two 4 GB UDIMM</i>	2	9 W
2.5-in SATA SSD (requires one additional chassis fan to cool disks)	1 to 4	Up to 8 W per SSD + 23 W for the fan required
50 W PCIe add-in card	1	54 W

**NOTICE**

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

## Network architecture

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

Table of contents

Once the network architecture is planned, go to sections [Baseboard management controller - BMC](#) to discover the management IP address and [Material, information and software required](#) to continue the planning.

Relevant sections:

[Product architecture](#)

## MAC addresses

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

Table of contents

- [Discovering the platform MAC addresses](#)
  - [Discovering a MAC address using the QR code](#)
  - [Discovering a MAC address using the BIOS](#)
    - [Accessing the BIOS using a serial console \(physical connection\)](#)
      - [Prerequisites](#)
      - [Port location](#)
      - [Access procedure](#)
    - [Accessing the BMC network configuration menu](#)

### ME1100 MAC addresses

Interface description	MAC address	Notes
BMC RJ45 port 3	MAC_BASE	Management: merged management/control plane
BMC SFP port 2	MAC_BASE + 1	Management: merged management/data plane
CPU RJ45 port 3	MAC_BASE + 2	Server control plane
CPU SFP port 1	MAC_BASE + 3	Server data plane
CPU SFP port 2	MAC_BASE + 4	Server data plane

## Discovering the platform MAC addresses

The platform MAC addresses can be discovered:

- Using the [QR code](#)
- Using the [BIOS](#)

### Discovering a MAC address using the QR code

Step_1	<p>Using a QR code application, scan the QR code. Record the information obtained in your device (e.g. by taking a screen shot).</p> <p>S/N:9017020001 = Platform serial number  P/N:1065-2823 = Platform part number  BATCH:0A00000001 = Platform production lot number  MAC:00A0A5D6402A = Platform BMC management MAC address</p>	<p>S/N: 9017020001  P/N: 1065-2823  BATCH: 0A00000001  MAC: 00A0A5D6402A</p>
--------	--	--

### Discovering a MAC address using the BIOS

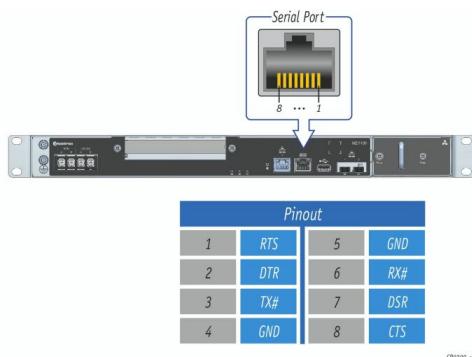
# PRELIMINARY

## Accessing the BIOS using a serial console (physical connection)

### Prerequisites

1	A physical connection to the device is required. <b>NOTE:</b> The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the external computer. <ul style="list-style-type: none"><li>• Speed (Baud): 115200</li><li>• Data bits: 8</li><li>• Stop bits: 1</li><li>• Parity: None</li><li>• Flow Control: None</li><li>• Recommended emulation mode: VT100+</li></ul> <b>NOTE:</b> PuTTY is recommended.

### Port location



### Access procedure

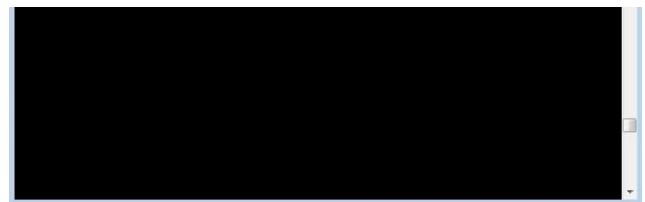
Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.
Step_2	Perform a server reset ( <b>Ctrl-break</b> hot key). <b>NOTE:</b> If an operating system is installed on the device, the hot key might not work properly. If this is the case, reset the server as recommended for the operating system. <b>NOTE:</b> When a server reset command is sent, it may take a few seconds for the BIOS sign on screen to display.
Step_3	When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu. <b>NOTE:</b> It may take a few seconds for the BIOS sign on screen to display confirmation message

COM12 - PuTTY  
System Information  
BOARD NAME BIOS Version: 2.10.0932F591 Date: "04/04/2019"  
Intel RC Version: 02.05.00  
CPU Info: Intel(R) Xeon(R) CPU D-1548 @ 2.00GHz  
Memory Info: Memory Size: 32GB Memory Speed: 2400MHz RAS Mode: Indep  
0x32 : CPU POST-Memory Initialization  
0x4F : DXE IPL Start  
0x68 : PCI HB Initialization.  
0x70 : SB DXE Initialization.  
0x79 : CSM Driver Entry point  
0x91 : Connecting Drivers.  
0x92 : PCI Bus Initialization.  
0x94 : PCI Bus Enumeration.  
0x94 : PCI Bus Request Resources.  
0x96 : PCI Bus Assign Resources.  
0x91 : Connecting Drivers.  
0x92 : PCI Bus Initialization.  
0x97 : Console Output devices connect.

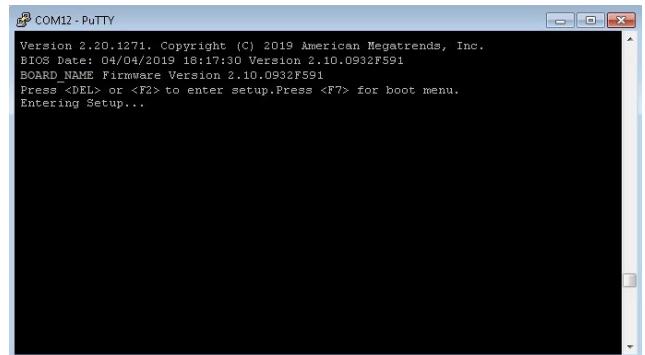
COM12 - PuTTY  
Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.  
BIOS Date: 04/04/2019 18:17:30 Version 2.10.0932F591  
BOARD\_NAME Firmware Version 2.10.0932F591  
Press <DEL> or <F2> to enter setup.Press <F7> for boot menu.  
"Entering Setup..."

## PRELIMINARY

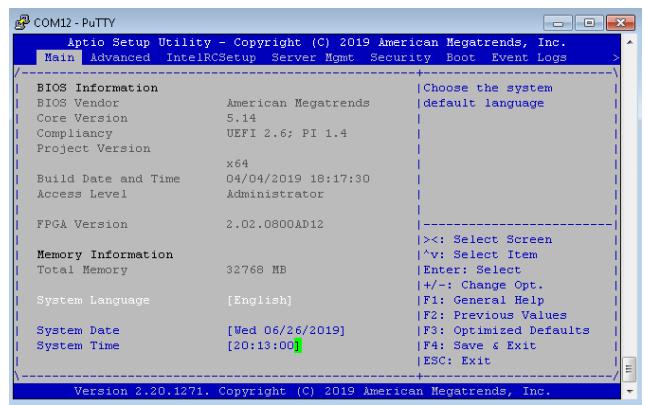
Entering Setup...



- Step\_4 The BIOS sign on screen displays "Entering Setup...".  
**NOTE:** It will take several seconds to display and enter the BIOS setup menu.

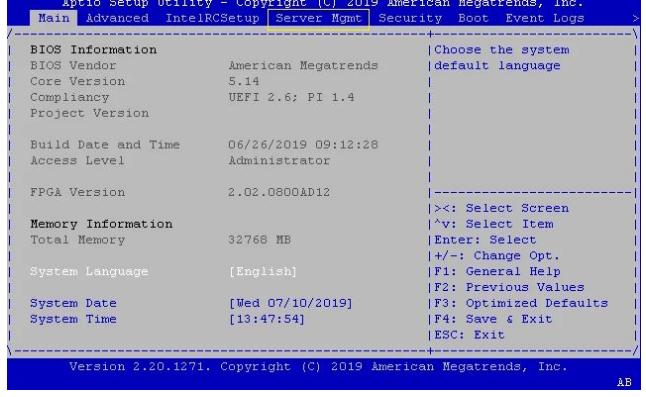
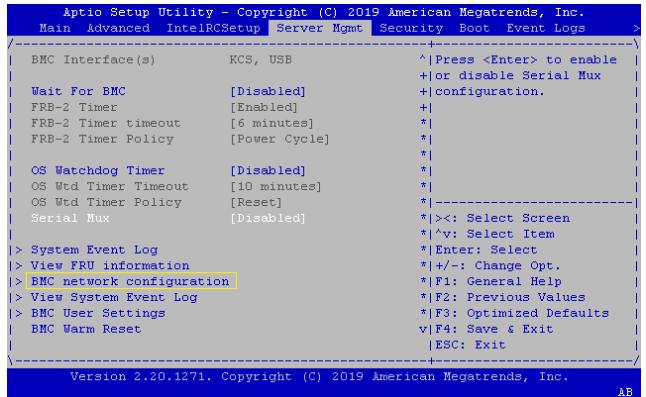
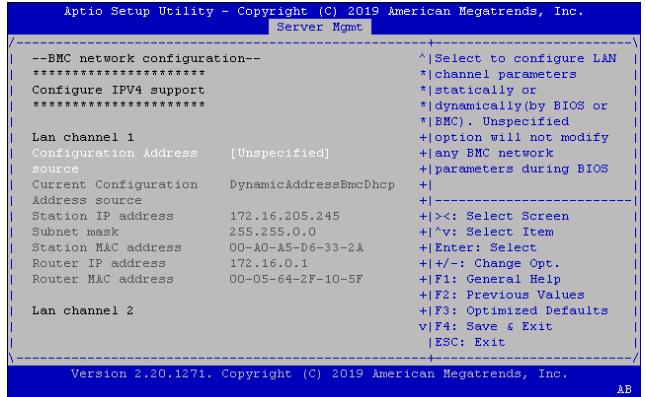


- Step\_5 The BIOS setup menu is displayed.



Accessing the BMC network configuration menu

# PRELIMINARY

Step_1	<p>From the BIOS menu, use the arrow keys to select <b>Server Mgmt</b>.</p>	 <p>The screenshot shows the Aptio Setup Utility main menu. The 'Server Mgmt' tab is highlighted in yellow. Other tabs include Main, Advanced, IntelRCSsetup, Security, Boot, and Event Logs. The BIOS information section displays details like BIOS Vendor (American Megatrends), Core Version (5.14), and System Date (Wed 07/10/2019). A legend at the bottom right provides keyboard shortcuts for navigation.</p>
Step_2	<p>Use the arrow keys to select <b>BMC network configuration</b>.</p>	 <p>The screenshot shows the BMC network configuration menu. The 'BMC network configuration' option is highlighted in yellow. Other options include BMC Interface(s) (KCS, USB), Wait For BMC (Disabled), OS Watchdog Timer (Disabled), and Serial Mux (Disabled). A legend at the bottom right provides keyboard shortcuts for navigation.</p>
Step_3	<p>The BMC network configuration menu is displayed.</p> <p><b>NOTE:</b> When the platform is powered up after being shut off, the BIOS may load before the BMC has received its IP address. In this case, the BIOS menu information will need to be refreshed by restarting the server and re-entering the BIOS.</p>	 <p>The screenshot shows the BMC network configuration menu. The 'BMC network configuration' option is highlighted in yellow. Other options include Configuration Address (Unspecified), Current Configuration (DynamicAddressBmcDhcp), and Router IP address (172.16.0.1). A legend at the bottom right provides keyboard shortcuts for navigation.</p>

## PCI mapping

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

Bus: Device. Function	Vendor ID	Device ID	Component	Description
00:00.0	8086	6F00	Host Bridge	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DMI2 (rev 03)
00:01.0	8086	6F02	PCI Bridge	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 1 (rev 03) (prog-if 00 [Normal decode])
00:01.1	8086	6F03	PCI bridge	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 1 (rev 03) (prog-if 00 [Normal decode])
00:02.0	8086	6F04	PCI Bridge	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 2 (rev 03) (prog-if 00 [Normal decode])
00:02.2	8086	6F06	PCI Bridge	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 2 (rev 03) (prog-if 00 [Normal decode])
00:03.0	8086	6F08	PCI Bridge	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 3 (rev 03) (prog-if 00 [Normal decode])
00:05.0	8086	6F28	System Peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Map/VTd_Misc/System Management (rev 03)
00:05.1	8086	6F29	System Peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Hot Plug (rev 03)
00:05.2	8086	6F2A	System Peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO RAS/Control Status/Global Errors (rev 03)
00:05.4	8086	6F2C	PIC	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D I/O APIC (rev 03) (prog-if 20 [IO(X)-APIC])
00:16.0	8086	8C3A	Communication Controller	Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller #1 (rev 04)
00:16.1	8086	8C3B	Communication Controller	Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller #2 (rev 04)
00:1c.0	8086	8c10	PCI bridge	Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #1 (rev d5) (prog-if 00 [Normal decode])
00:1c.4	8086	8c18	PCI bridge	Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #5 (rev d5) (prog-if 00 [Normal decode])
00:1D.0	8086	8C26	USB Controller	Intel Corporation 8 Series/C220 Series Chipset Family USB EHCI #1 (rev 05) (prog-if 20 [EHCI])
00:1F.0	8086	8C54	ISA Bridge	Intel Corporation C224 Series Chipset Family Server Standard SKU LPC Controller (rev 05)
00:1F.2	8086	8C02	SATA Controller	Intel Corporation 8 Series/C220 Series Chipset Family 6-port SATA Controller 1 [AHCI mode] (rev 05) (prog-if 01 [AHCI 1.0])
00:1F.3	8086	8C22	SMBus	Intel Corporation 8 Series/C220 Series Chipset Family SMBus Controller (rev 05)
03:00.0	8086	6F50	System Peripheral	Intel Corporation Xeon Processor D Family QuickData

# PRELIMINARY

03:00.0	8086	6F50	System Peripheral	Intel Corporation Xeon Processor D Family QuickData Technology Register DMA Channel 0
03:00.1	8086	6F51	System Peripheral	Intel Corporation Xeon Processor D Family QuickData Technology Register DMA Channel 1
03:00.2	8086	6F52	System Peripheral	Intel Corporation Xeon Processor D Family QuickData Technology Register DMA Channel 2
03:00.3	8086	6F53	System Peripheral	Intel Corporation Xeon Processor D Family QuickData Technology Register DMA Channel 3
04:00.0	8086	15AC	Ethernet Controller	Intel Corporation Ethernet Connection X552 10 GbE SFP+
04:00.1	8086	15AC	Ethernet Controller	Intel Corporation Ethernet Connection X552 10 GbE SFP+
07:00.0	1A03	1150	PCI bridge	ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge (rev 04) (prog-if 00 [Normal decode])
08:00.0	1A03	2000	VGA compatible controller	ASPEED Technology, Inc. ASPEED Graphics Family (rev 41) (prog-if 00 [VGA controller])
09:00.0	8086	1533	Ethernet controller	Intel Corporation I210 Gigabit Network Connection (rev 03)
FF:0B.0	8086	6F81	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R3 QPI Link 0/1 (rev 03)
FF:0B.1	8086	6F36	Performance counters	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R3 QPI Link 0/1 (rev 03)
FF:0B.2	8086	6F37	Performance counters	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R3 QPI Link 0/1 (rev 03)
FF:0B.3	8086	6F76	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R3 QPI Link Debug (rev 03)
FF:0C.0	8086	6FE0	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0C.1	8086	6FE1	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0C.2	8086	6FE2	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0C.3	8086	6FE3	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0C.4	8086	6FE4	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0C.5	8086	6FE5	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0C.6	8086	6FE6	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0C.7	8086	6FE7	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0F.0	8086	6FF8	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0F.4	8086	6FFC	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)

## PRELIMINARY

FF:0F.5	8086	6FFD	System peripheral	Intel Corporation Xeon E / v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:0F.6	8086	6FFE	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 03)
FF:10.0	8086	6F1D	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R2PCIe Agent (rev 03)
FF:10.1	8086	6F34	Performance counters	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R2PCIe Agent (rev 03)
FF:10.5	8086	6F1E	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Ubox (rev 03)
FF:10.6	8086	6F7D	Performance counters	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Ubox (rev 03)
FF:10.7	8086	6F1F	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Ubox (rev 03)
FF:12.0	8086	6FA0	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Home Agent 0 (rev 03)
FF:12.1	8086	6F30	Performance counters	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Home Agent 0 (rev 03)
FF:13.0	8086	6FA8	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Target Address/Thermal/RAS (rev 03)
FF:13.1	8086	6F71	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Target Address/Thermal/RAS (rev 03)
FF:13.2	8086	6FAA	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel Target Address Decoder (rev 03)
FF:13.3	8086	6FAB	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel Target Address Decoder (rev 03)
FF:13.4	8086	6FAC	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel Target Address Decoder (rev 03)
FF:13.5	8086	6FAD	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel Target Address Decoder (rev 03)
FF:13.6	8086	6FAE	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Broadcast (rev 03)
FF:13.7	8086	6FAF	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Global Broadcast (rev 03)
FF:14.0	8086	6FB0	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 0 Thermal Control (rev 03)
FF:14.1	8086	6FB1	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 1 Thermal Control (rev 03)
FF:14.2	8086	6FB2	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 0 Error (rev 03)
FF:14.3	8086	6FB3	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 1 Error (rev 03)
FF:14.4	8086	6FBC	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Interface (rev 03)
FF:14.5	8086	6FBD	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Interface (rev 03)

## PRELIMINARY

FF:14.6	8086	6FBE	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Interface (rev 03)
FF:14.7	8086	6FBF	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Interface (rev 03)
FF:15.0	8086	6FB4	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 2 Thermal Control (rev 03)
FF:15.1	8086	6FB5	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 3 Thermal Control (rev 03)
FF:15.2	8086	6FB6	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 2 Error (rev 03)
FF:15.3	8086	6FB7	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 3 Error (rev 03)
FF:1E.0	8086	6F98	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 03)
FF:1E.1	8086	6F99	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 03)
FF:1E.2	8086	6F9A	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 03)
FF:1E.3	8086	6FC0	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 03)
FF:1E.4	8086	6F9C	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 03)
FF:1F.0	8086	6F88	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 03)
FF:1F.2	8086	6F8A	System peripheral	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 03)

## Platform, modules and accessories

*{This article provides the complete list of compatible parts and components that can be ordered from Kontron.}*

Description	Kontron P/N
Fan tray assembly (3 fans with filter)	1062-7023
Fan tray assembly (4 fans with filter)	1065-0085
Fan filter assembly	1066-4009
RJ45 to DB9 serial adaptor	1015-9404
C13 to CEE 7/7 European AC power cord, 10A/250 VAC, 1.8m long	1061-0410
C13 to NEMA 5-15P AC power cord, 10A/125 VAC, 2m long	1-340000-0
Ground lug right angle, 8 AWG	1064-4226
Thermal probe for PCIe add-in card	1065-9296
ME1100 with CPU Xeon D-1548, DC input, no memory, no storage	1065-2823
ME1100 with CPU Xeon D-1567, DC input, no memory, no storage	1065-2824
ME1100 with CPU Xeon D-1559, DC input, no memory, no storage	1065-2825
ME1100 with CPU Xeon D-1567, DC input,,16GB UDIMM memory, 32GB M.2 SSD SATA	1065-6327
ME1100 with CPU Xeon D-1548, AC input, no memory, no storage	1065-2916
ME1100 with CPU Xeon D-1567, AC input, no memory, no storage	1065-2917
ME1100 with CPU Xeon D-1559, AC input, no memory, no storage	1065-2919

# Material, information and software required

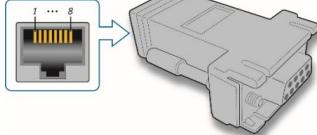
*{This article details the material, information and software required for proper configuration and deployment.}*

## Table of contents

- [Optional adapter](#)
- [PCIe add-in card](#)
- [DC Power cables and tooling](#)
- [Rack installation material](#)
- [Network cables and modules](#)
- [Network infrastructure](#)
- [Software required](#)

## Material and information required

### Optional adapter

Item_1	<p>RJ45 to DB9 serial adapter (Kontron P/N: 1015-9404)</p>  <table border="1" style="margin-top: 10px; border-collapse: collapse; text-align: center;"> <thead> <tr> <th colspan="8">Pinout</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> <p style="font-size: small; margin-top: 5px;">C9055A</p>	Pinout								1	RTS	5	GND	2	DTR	6	RX#	3	TX#	7	DSR	4	GND	8	CTS
Pinout																									
1	RTS	5	GND																						
2	DTR	6	RX#																						
3	TX#	7	DSR																						
4	GND	8	CTS																						

### PCIe add-in card

Item_1	One T8 Torx screwdriver
Item_2	One 3-mm flat-head screwdriver
Item_3	One T10 Torx screwdriver
Item_4	One tie wrap, if the PCIe add-in card is a FH3/4L
Item_5	One thermal probe for temperature monitoring (if physical temperature monitoring is chosen)

### DC Power cables and tooling

## PRELIMINARY

Item_1	Crimp lugs: <ul style="list-style-type: none"> <li>• 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)</li> </ul>
Item_2	Black stranded wire to build the power cable based on the length required: <ul style="list-style-type: none"> <li>• 14 AWG insulation diameter max.: 4.40 mm [0.175 in] for Molex crimp lugs OR • 12 AWG insulation diameter max.: 5.8 mm [0.23 in] for Panduit crimp lugs</li> </ul>
Item_3	Red stranded wire to build the power cable based on the length required: <ul style="list-style-type: none"> <li>• 14 AWG insulation diameter max.: 4.40 mm [0.175 in] for Molex crimp lug OR • 12 AWG insulation diameter max.: 5.8 mm [0.23 in] for Panduit crimp lug</li> </ul>
Item_4	One hand crimp tool: <ul style="list-style-type: none"> <li>• Molex Premium Grade Hand Crimp Tool (640010100) OR • Panduit Hand Crimp Tool (638130400)</li> </ul>
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	8 mm wrench or equivalent tool

### Rack installation material

Item_1	Racking fasteners (rack specific)
--------	-----------------------------------

### Network cables and modules

Relevant section:

[Hardware compatibility list](#)

Item_1	One SFP or SFP+ data plane module and cable <ul style="list-style-type: none"> <li>• SFP/SFP+ optical modules (SX, LX, SR, LR) with compatible optical cable</li> </ul>
Item_2	One RJ45 Ethernet management plane cable
Item_3	One RJ45 serial connection cable

### Network infrastructure

- IP addresses:
  - One management plane IP
  - Up to 2 data plane IPs

Relevant sections:

[Platform, modules and accessories](#)

[Hardware compatibility list](#)

## Software required

Item_1	A community version of <b>ipmitool</b> is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.
Item_2	A terminal emulator such as <b>puTTY</b> is installed on a remote computer.
Item_3	A hardware detection tool such as <b>pciutils</b> is installed on the local server to view information about devices connected to the server PCI buses .

## Hardware compatibility list

*(This article provides the list of qualified and compatible hardware components.)*

### Table of contents

- [M.2-2280 industrial SSD \(-40°C to 85°C\)](#)
- [2.5-in industrial SSD drives \(-40°C to 85°C\)](#)
- [SFP and SFP+ industrial modules \(-40°C to 85°C\)](#)

### DDR4 industrial memory (-40°C to 85°C)

Manufacturer	Manufacturer P/N	Type	Size	Description	Status	Kontron P/N
Innodisk	M4C0-4GSSLWSJ-U48	UDIMM	4 GB	DDR4-2133/2400 ECC	Active	1065-6675
ATP	A4C04QV8BLTDSW	UDIMM	4 GB	DDR4-2133/2400 ECC	Active	
Innodisk	M4C0-8GSSMWSJ-U48	UDIMM	8 GB	DDR4-2133/2400 ECC	Active	1065-5815
ATP	A4C08QV8BNTDMW	UDIMM	8 GB	DDR4-2133/2400 ECC	Active	
Transcend	TS1GLH72V6B-I	UDIMM	8 GB	DDR4-2133/2400/2666 ECC	Active	1065-6771
Innodisk	M4C0-AGS1MWSJ-U48	UDIMM	16 GB	DDR4-2133/2400 ECC	Active	
ATP	A4C16QW8BNTDMW	UDIMM	16 GB	DDR4-2133/2400 ECC	Active	1065-7666
Transcend	TS2GLH72V6B-I	UDIMM	16 GB	DDR4-2133/2400/2666 ECC	Active	
ATP	X4B32QJ4DVRCWSW	RDIMM	32 GB	DDR4-2133/2400 ECC	Active	1065-7666

### M.2-2280 industrial SSD (-40°C to 85°C)

Manufacturer	Manufacturer P/N	Type	Size	Status	Kontron P/N
Innodisk	DEM28-32GM41BW1DC-U48	SATA	32 GB	Active	1065-5798
Transcend	TS32GMTS800I	SATA	32 GB	Active	
Innodisk	DEM28-A28M41BW1DC-U48	SATA	128 GB	Active	1065-7669
ATP	AF128GSMIC-VABIP	SATA	128 GB	Active	
Transcend	TS128GMTS800I	SATA	128 GB	Active	1065-7935
Innodisk	DGM28-C12D81BWBQC-U48	SATA	512 GB	Active	
ATP	AF512GSMIC-VABIP	SATA	512 GB	Active	1065-8190
Transcend	TS512GMTS800I	SATA	512 GB	Active	
ATP	AF1TSMIC-VABIP	SATA	1 TB	Active	1065-8190
Transcend	TS1TMTS800I	SATA	1 TB	Active	
Innodisk	DGM28-01TD81BWBQC-U48	SATA	1 TB	Active	

# PRELIMINARY

## 2.5-in industrial SSD drives (-40°C to 85°C)

Manufacturer	Manufacturer P/N	Type	Size	Status	Kontron P/N
Innодиск	DES25-C12DK1EW3QF-U48	SATA III (6.0Gb/S) 7mm	512 GB	Active	1065-8263
ATP	AF512GSMCJ-VABIP	SATA III (6.0Gb/S) 9mm	512 GB	Active	
Transcend	TS512GSSD420I	SATA III (6.0Gb/S) 7mm	512 GB	Active	

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

Manufacturer	Manufacturer P/N	Protocol	Description	Status	Kontron P/N
Finisar	FTLF8519P3BTL	1000BASE-SX	500m, 850nm, -40°C to 85°C, SFP optical transceiver	Active	1064-5770
Finisar	FTLX8573D3BTL	10GBASE-SR	400m, 850nm, -40°C to 85°C, SFP+ optical transceiver	Active	1064-5765
FormericaOE	TAS-A2NH1-P11	10GBASE-SR	300m, 850nm, -40°C to 85°C, SFP+ optical transceiver	Active	
FormericaOE	TSD-S2CA1-F11	1000BASE-LX	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	1065-3758
Finisar	FTLF1318P3BTL	1000BASE-LX	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	
Avago	AFCT-5715ALZ	1000BASE-LX	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	
FS	SFP-10GLR-31	10GBASE-LR	10Km, 1310nm, -40°C to 85°C, SFP+ optical transceiver	Active	1065-6804
Finisar	FTLX1475D3BTL	10GBASE-LR	10Km, 1310nm, -40°C to 85°C, SFP+ optical transceiver	Active	

# Validated operating systems

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

Table of contents

- [Status description](#)
- [OS certification status](#)

## Status description

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

## OS certification status

Operating system	Status	Links
SUSE® SLES 12 SP5	IN PROCESS	
SUSE® SLES 15	PLANNED	
Ubuntu Server LTS 16.04	VALIDATED	
Ubuntu Server LTS 18.04	VALIDATED	
VMware 7.0	PLANNED	
VMware 6.7	CERTIFIED	<a href="https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=server&amp;productId=50040&amp;deviceCategory=server&amp;details=1&amp;keyword=%">https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=server&amp;productId=50040&amp;deviceCategory=server&amp;details=1&amp;keyword=%</a>
RHEL 7.7	CERTIFIED	<a href="https://access.redhat.com/ecosystem/hardware/3624391">https://access.redhat.com/ecosystem/hardware/3624391</a>
RHEL 7.5	CERTIFIED	<a href="https://access.redhat.com/ecosystem/hardware/3624391">https://access.redhat.com/ecosystem/hardware/3624391</a>
CentOS 7.4	VALIDATED	

## Security

{This article provides information and guidance on best practices to adopt in order to insure security.}

- Establish a plan to change default user names and password. Refer to [Configuring and managing users](#).
- Determine the access paths that are to be closed or open. Refer to [Configuring system access methods](#).
- The platform features a Trusted Platform Module (TPM). Determine your requirement with regards to hardware-based, security-related functions. Refer to [Configuring TPM](#).

For more information on security features, contact Kontron.

## Installing

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

Children

- [Mechanical installation and precautions](#)
  - [ESD protections](#)
  - [Unboxing](#)
  - [Component installation and assembly](#)
  - [Airflow](#)
  - [Rack installation](#)
  - [Cabling](#)
- [Software installation and deployment](#)
  - [Preparing for installation](#)
  - [Installing an operating system on a server](#)
  - [Verifying installation](#)
  - [Content under creation] Platform installation for high availability
  - [Common software installation](#)

## Mechanical installation and precautions

{This section details the steps and safety precautions required for the physical installation of the product.}

Children

- [ESD protections](#)
- [Unboxing](#)
- [Component installation and assembly](#)
- [Airflow](#)
- [Rack installation](#)
- [Cabling](#)

## ESD protections

*{This article provides guidelines regarding ESD protection.}*

Electrostatic discharge ( ESD) can damage electronic components (e.g., disk drives and boards).

Look for this warning in the documentation as it indicates that the device is ESD sensitive and that precautions must be taken.



### ESD sensitive device!

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

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

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

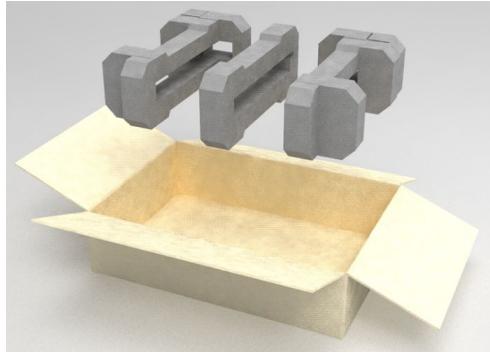
## Unboxing

*{This article gives specific instructions to safely unbox the product and to validate the bill of materials.}*

---

### What's in the box

The ME1100 platform box includes one ME1100 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.

## Component installation and assembly

{This article provides detailed instructions to safely assemble and install optional components.}

### Table of contents

- [Opening the enclosure](#)
- [Installing an optional PCIe add-in card](#)
  - [Adjusting the PCIe length](#)
  - [Connecting the PCIe add-in card](#)
- [Installing an M.2 storage](#)
  - [Locating the M.2 storage](#)
  - [Installing the M.2 storage](#)
- [Installing DIMMs](#)
  - [Locating the DIMMs](#)
  - [Installing a DIMM](#)
- [Replacing an SSD](#)
- [Installing a thermal probe for the PCIe add-in card](#)
  - [Locating the thermal probe connection](#)
  - [\(Optional\) Building a thermal probe](#)
  - [Installing the thermal probe](#)
- [Closing the enclosure](#)
- [Replacing a fan tray assembly](#)



#### 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.



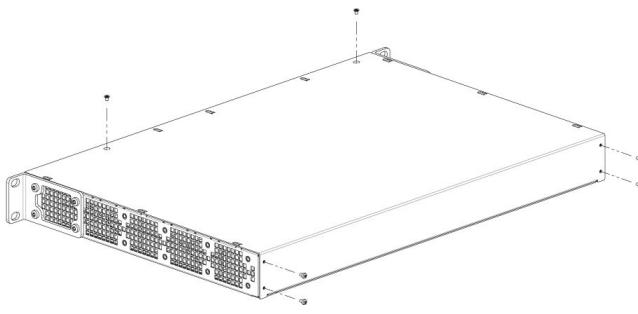
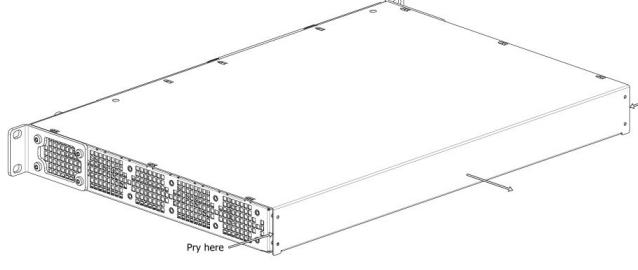
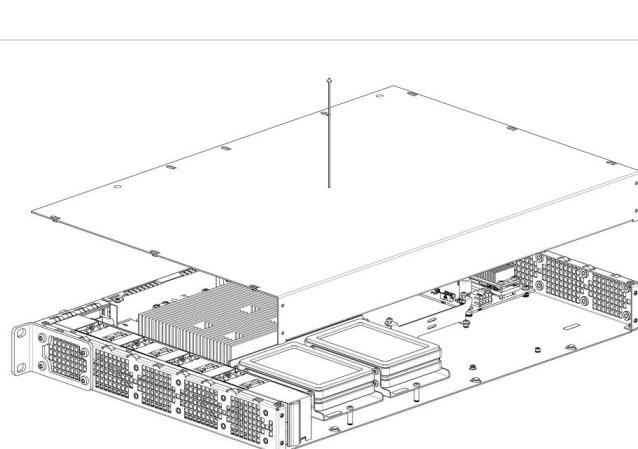
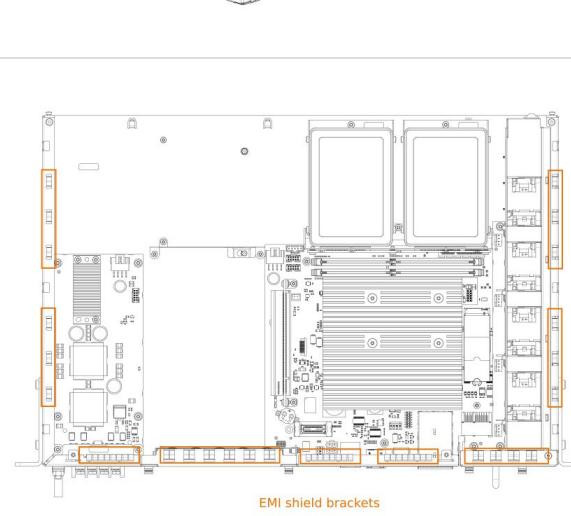
When handling components, follow the precautions described in section [ESD protections](#).



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

## Opening the enclosure

## PRELIMINARY

Step_1	Remove the 4 screws in the back using a T8 Torx screwdriver.	
Step_2	Remove the 2 screws on top using a T8 Torx screwdriver .	
Step_3	On both sides of the unit, insert a flat-head screwdriver in the cavity shown, and slightly slide the cover to the back to release it.	
Step_4	Apply pressure on the cover with your hands to release it from the casing.	
Step_5	Make sure the EMI shield brackets are in their appropriate position. They should not fall in the chassis.	

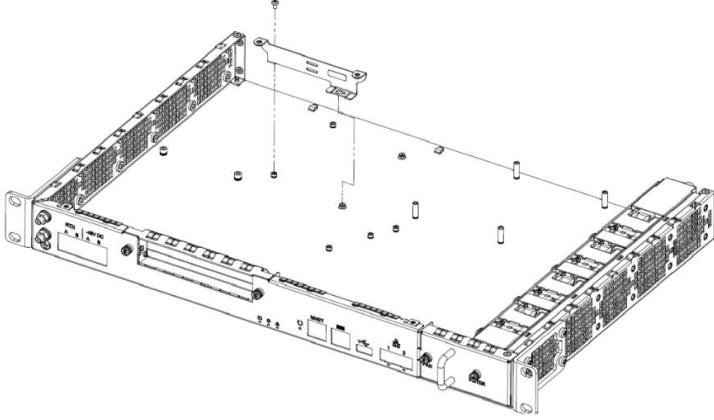
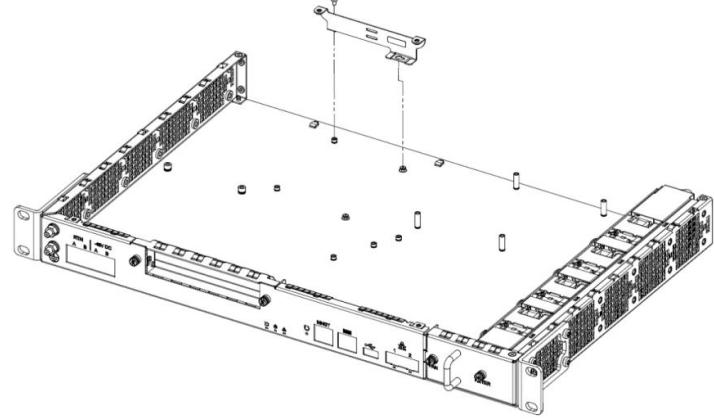
## Installing an optional PCIe add-in card

### Adjusting the PCIe length

## PRELIMINARY

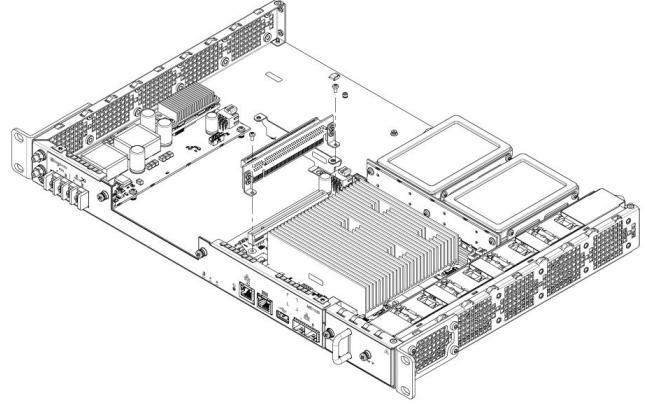
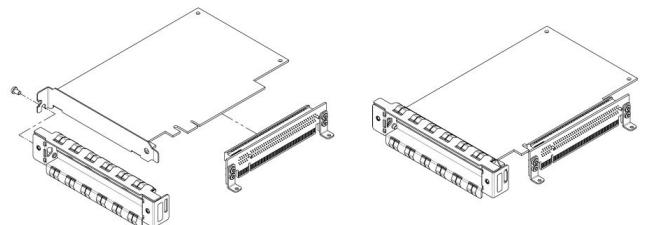
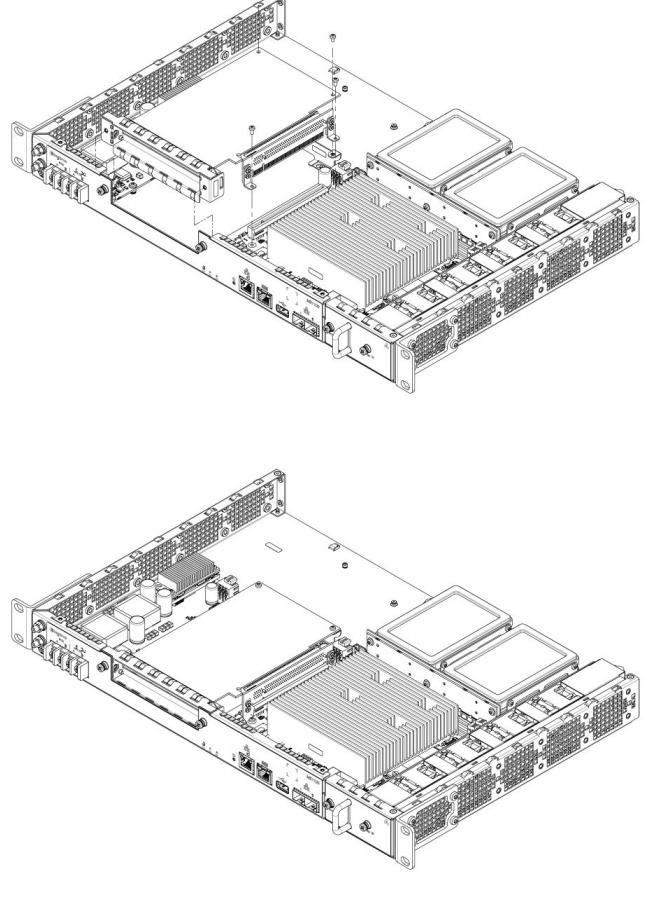
The maximum form factor of the optional PCIe add-in card is full-height, three-quarter length (FH3/4L).  
A T10 Torx screwdriver, scissors and a tie wrap are required.

**NOTE:** In this example, the rear mounting bracket is moved from half length to three-quarter length.

Step_1	Cut the tie wrap holding the power cable. Be careful not to cut one of the wires.	
Step_2	Remove the PCIe rear mounting bracket from the enclosure by removing the screw with a T8 Torx screwdriver.	
Step_3	Move the PCIe rear mounting bracket to the desired position and fasten the screw with a T8 Torx screwdriver .	
Step_4	Reattach the power cable using a tie wrap as shown in the picture.	

### Connecting the PCIe add-in card

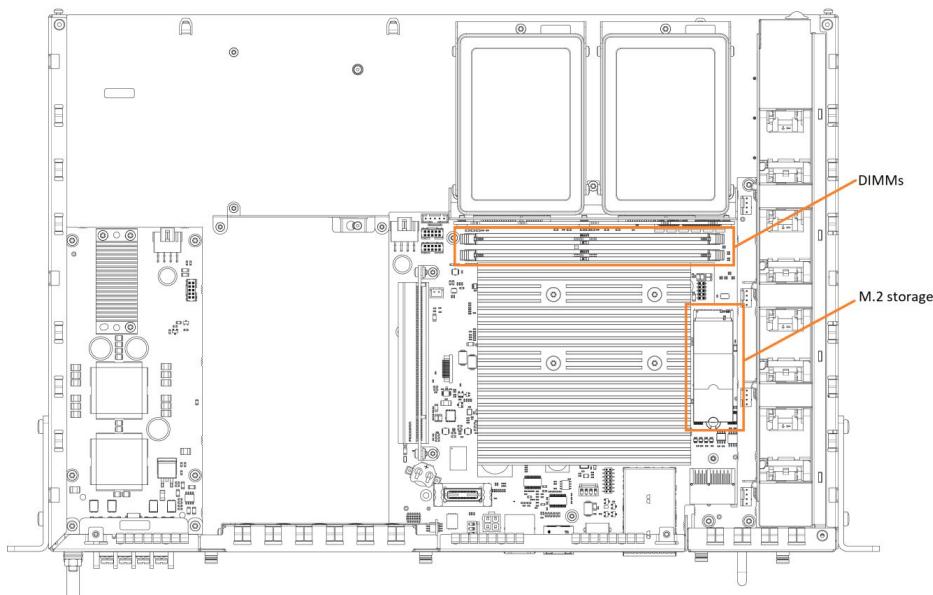
## PRELIMINARY

<p><b>Step_1</b></p> <p>Disconnect the PCIe riser by removing the 2 screws with a T8 Torx screwdriver.</p>	
<p><b>Step_2</b></p> <p>Install the PCIe add-in card onto the PCIe riser. Mount the front plate adapter onto the PCIe add-in card's L-bracket. Fasten the front plate adapter screw to the L-bracket using a T10 Torx screwdriver (6 lbf·in torque).</p>	
<p><b>Step_3</b></p> <p>Remove the 2 mounting screws from the rear mounting bracket using a T8 Torx screwdriver. Carefully insert the PCIe add-in card assembly into the unit by fastening the following 6 screws:</p> <ul style="list-style-type: none"> <li>• 2 T8 Torx screws for the riser card onto the server motherboard (4 lbf·in torque)</li> <li>• 2 T8 Torx screws for the PCIe add-in card into the rear mounting bracket (4 lbf·in torque)</li> <li>• 2 T10 Torx captive screws into the front plate (6 lbf·in torque)</li> </ul>	

## Installing an M.2 storage

### Locating the M.2 storage

# PRELIMINARY



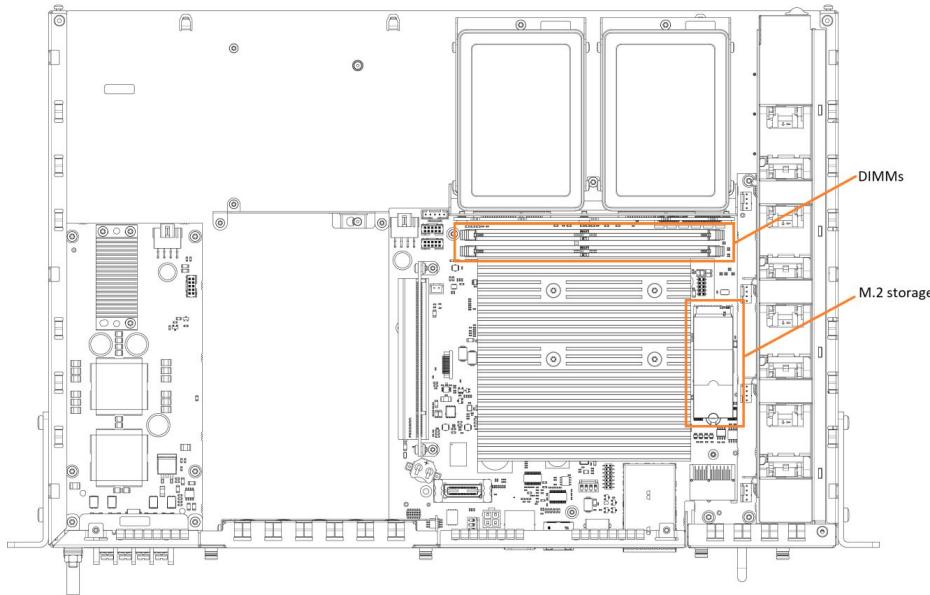
## Installing the M.2 storage

Only one M.2 SSD storage device can be installed per chassis.

Step_1	Remove the screw and washer from the bottom section with a T6 Torx screwdriver.	<p>A diagram showing a flat metal plate or bracket. A screw and washer are being removed from a hole in the center of the plate. Dashed lines indicate the path of the screw and washer as they are being taken out.</p>
Step_2	Insert the M.2 storage into the connector as prescribed in the M.2 specifications.	<p>A diagram showing a flat metal plate or bracket. An M.2 SSD is being inserted into a connector on the plate. A dashed line indicates the path of the SSD as it is being pushed into place.</p>
Step_3	Put the screw and washer back in place and tighten (2 lbf-in torque).	<p>A diagram showing a flat metal plate or bracket. The screw and washer are being reattached to the same hole where they were removed. Dashed lines indicate the path of the screw and washer as they are being put back in place.</p>

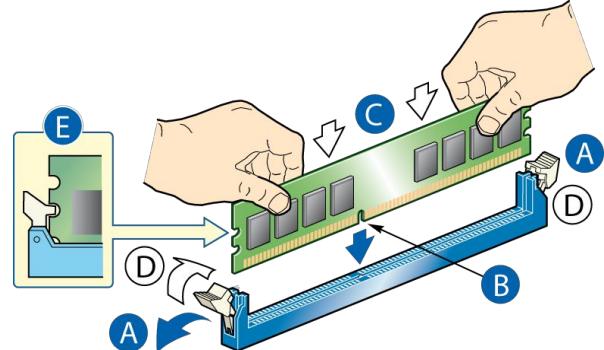
# Installing DIMMs

## Locating the DIMMs



## Installing a DIMM

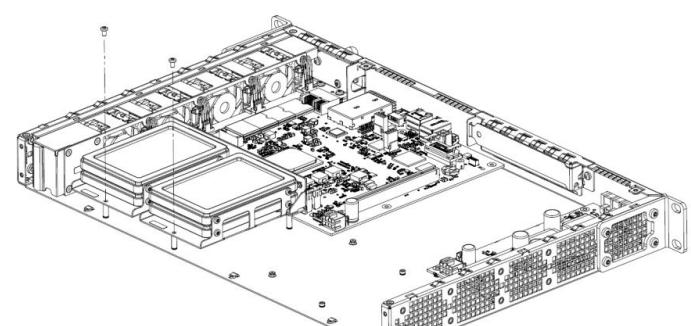
Step_1	Open the levers of the DIMM slot. (A)
Step_2	Note the location of the alignment notch on the DIMM edge. (B)
Step_3	Insert the DIMM, making sure the connector edge of the DIMM aligns correctly with the slot. (E)
Step_4	Using both hands, push down firmly and evenly on both sides of the DIMM until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



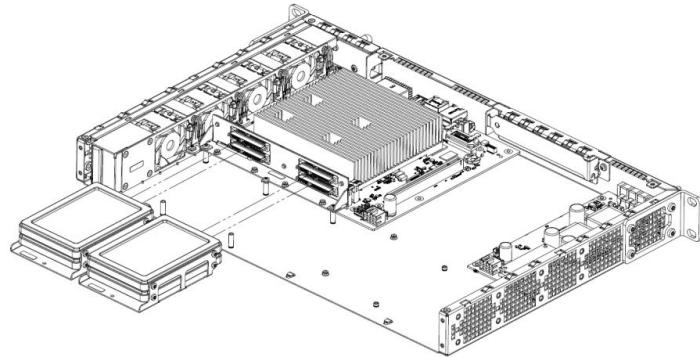
## Replacing an SSD

Up to four 2.5-in SSDs can be installed in the server as an option.

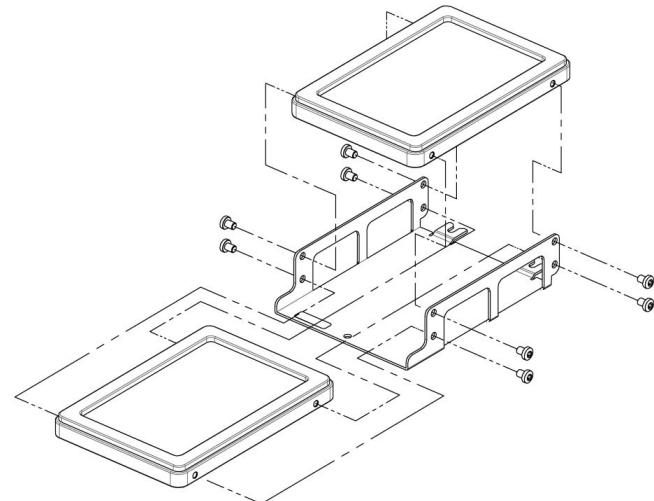
Step_1	Remove the two T10 Torx screws holding the two carrier brackets .
--------	---



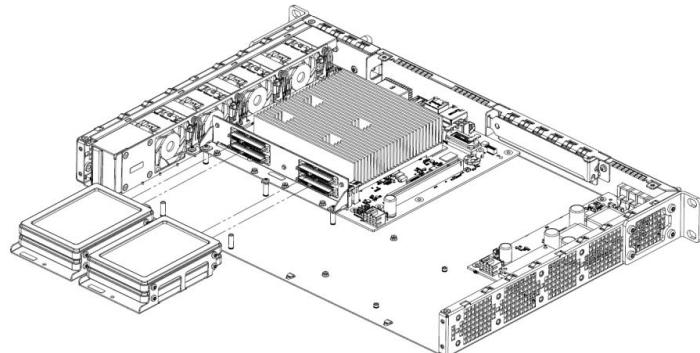
**Step\_2** Slide the carrier brackets containing the 2.5-in SSDs out of the chassis.



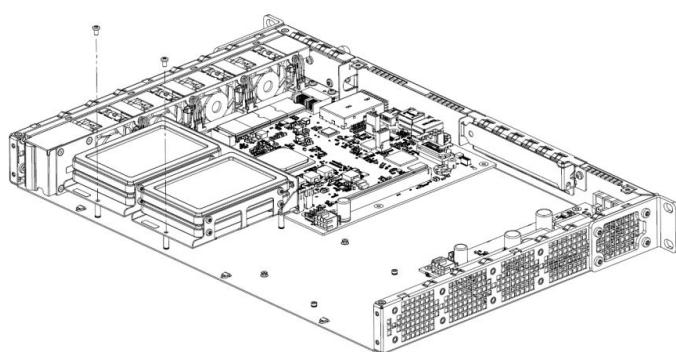
**Step\_3** Remove the 4 T10 Torx screws holding each 2.5-in SSD. Replace one or more 2.5-in SSD. Fasten each 2.5-in SSD in an SSD carrier bracket using 4 T10 Torx screws (2 lbf-in torque). Two 2.5-in SSD drives can be installed in one carrier bracket.



**Step\_4** Slide the carrier brackets containing the 2.5-in SSDs into the SSD rear mounting bracket.

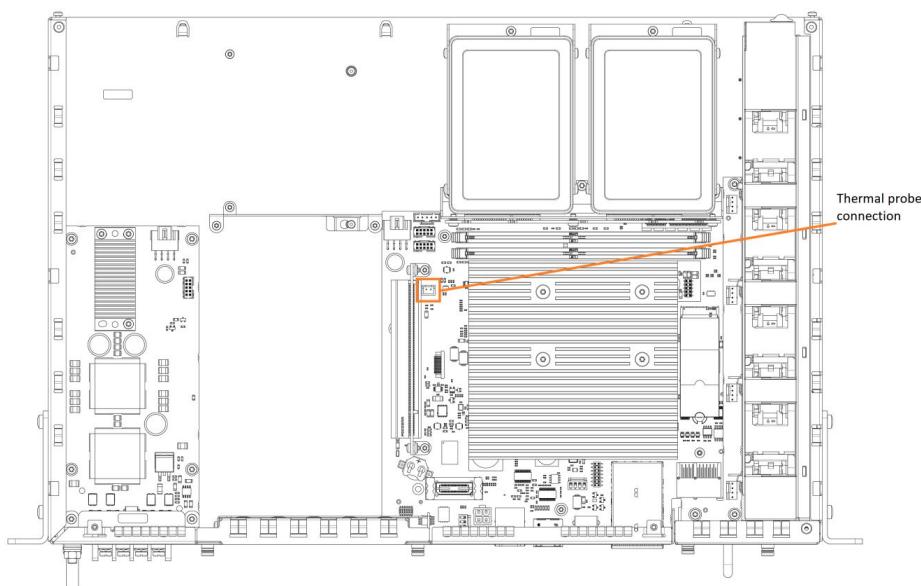


**Step\_5** Fasten each carrier bracket with one T10 Torx screw (6 lbf-in torque).



## Installing a thermal probe for the PCIe add-in card

### Locating the thermal probe connection



## (Optional) Building a thermal probe

A thermal probe can be purchased from Kontron or built.

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

Step_1	Using the components described in the table above, build a thermal probe.
--------	---

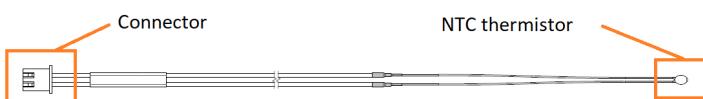
## Installing the thermal probe

Relevant sections:

[Managing customer added sensors](#)

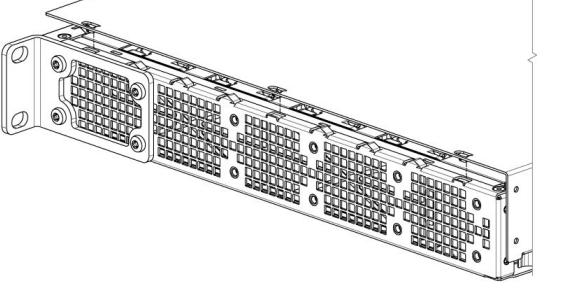
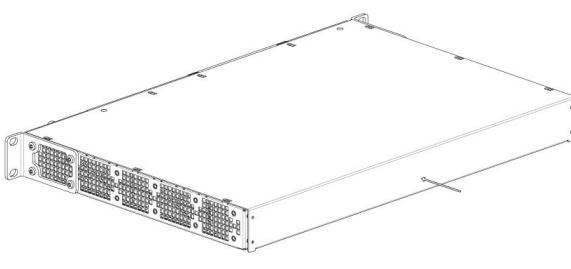
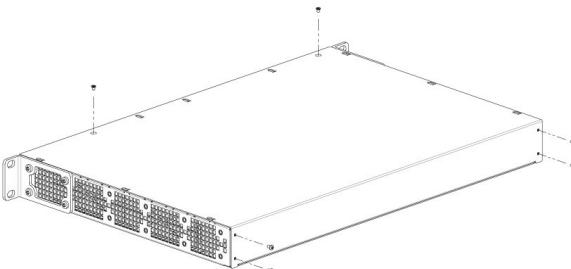
[Platform cooling and thermal management](#)

[Monitoring sensors](#)



Step_1	Install the thermal probe in the connector as prescribed in the thermal probe specifications.
Step_2	<p>Affix the NTC thermistor to the PCIe card.</p> <p>Typically, thermistors are installed between the fins of the PCIe card heatsink. Do not forget to use glue that can withstand the temperature.</p> <p><b>NOTE:</b> Configuration will be performed once the platform is operational (thresholds, specific software configurations, etc.).</p>

## Closing the enclosure

Step_1	<p>Align the cover lock mechanisms with the cutouts on the chassis and slide it toward the front to fasten it into place.</p>	 
Step_2	<p>Insert the 4 T8 Torx screws in the back and the 2 T8 Torx screws on top without turning them, making sure the holes on the cover and the holes on the chassis are properly aligned.  <b>NOTE:</b> Tightening screws into unaligned holes will damage the threads.</p>	
Step_3	<p>Tighten the 6 screws using a T8 Torx screwdriver to lock the cover in place.</p>	

## Replacing a fan tray assembly

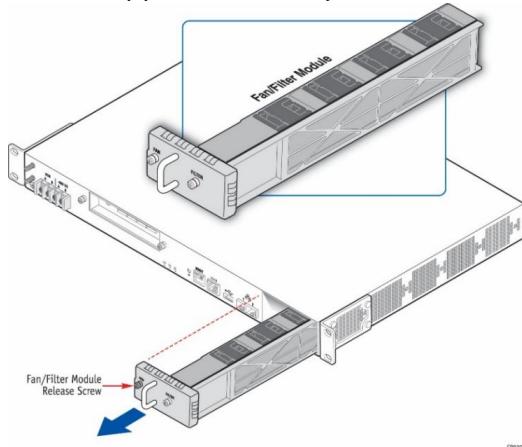
The ME1100 platform is equipped with a fan tray assembly comprised of fans and a filter. The filter can be pulled out by itself or the entire fan tray assembly (i.e., the fans and the filter) can be pulled out.

- To service the entire fan tray: unfasten the fan screw.
- To service the filter only: unfasten the filter screw and clean using oil-free compressed air.

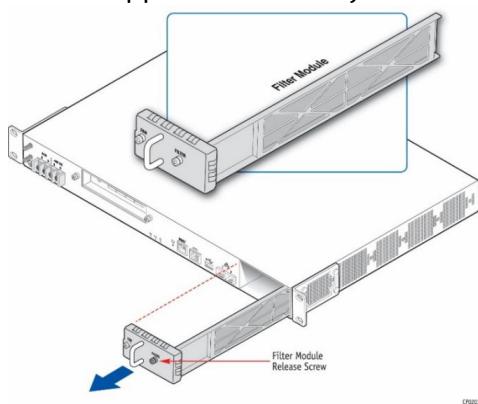
# PRELIMINARY

<b>⚠WARNING</b>	Always replace the fan tray with the equivalent fan tray assembly (part number). Two fan tray kits are available for the ME1100 product. Fan tray with 3 fans (standard) and fan tray with 4 fans when ME1100 is configured with 2.5-in SSDs. Using the wrong fan tray may cause thermal issues in the system.
<b>⚠WARNING</b>	Fan air filter should be inspected on a regular basis, based on the environment of their location. The inspection could be required every 2 years (in a very clean environment) or even every 3 months (in a slightly dusted environment). It is recommended that 3 months after the first installation, an inspection is executed in order to assess the ?state? of the filter. Base on how the filter is clogged, the schedule for cleaning or replacement of the filter can be established. Note that for installation done according to Telcordia NEBS requirements, filters must be replaced (R4-27 [145]) they cannot be cleaned. For other type of installation, filters could be cleaned up to 3 times, after what they must be replaced. It is recommended to replace filter every 3 years, replacement is required before residual dust build-up and provide air flow resistance. To clean filter you can use slightly compressed air, vacuum, and/or rinsed them with clean water. If water is use make sure the filter is completely dry before reinstalling

Hot-swappable fan tray



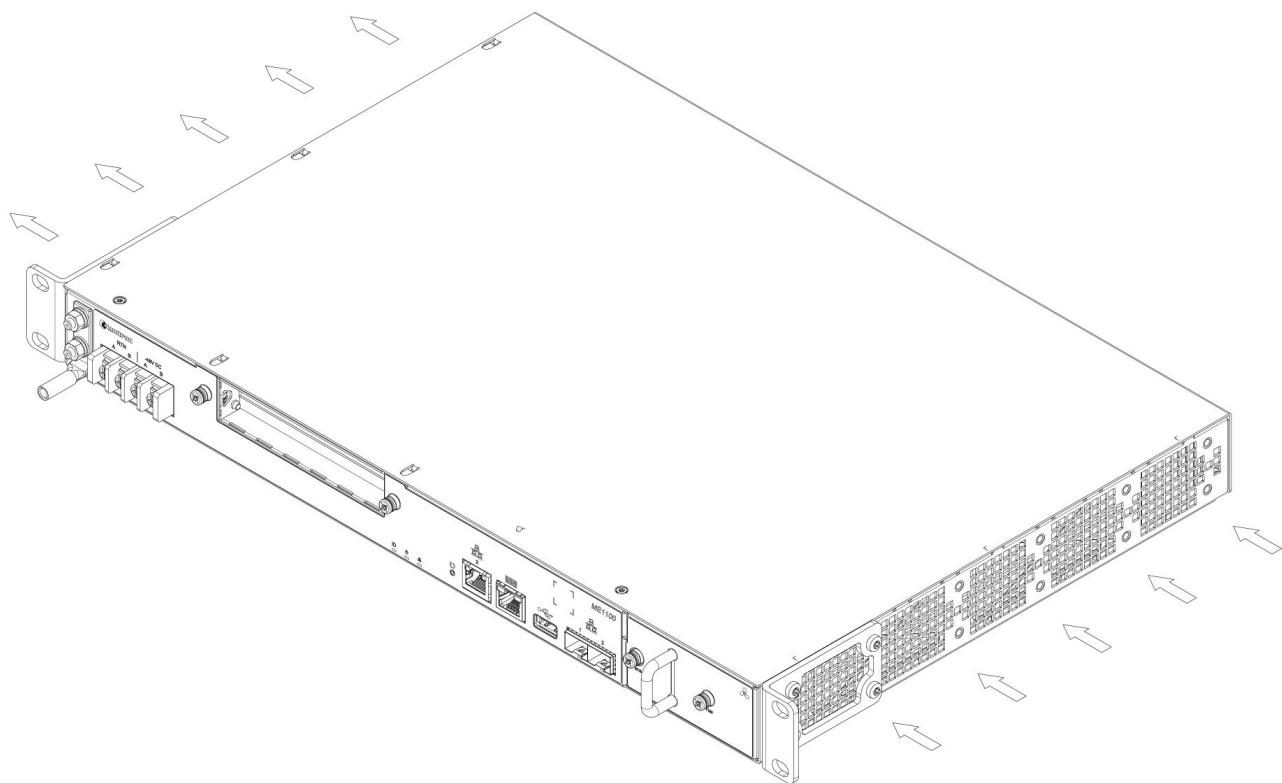
Hot-swappable filter tray



## Airflow

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

---



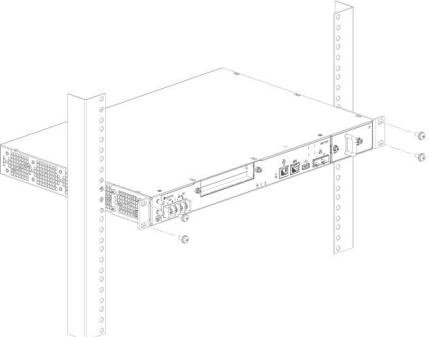
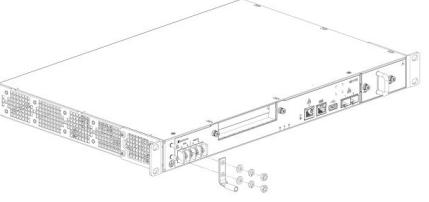
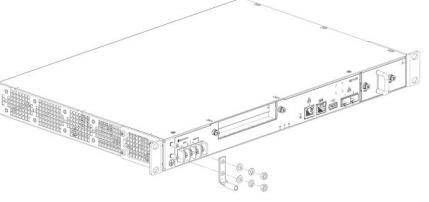
## Rack installation

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

Table of contents

### Installing an ME1100 platform in a 19-in rack

The airflow of the platform goes from right to left, facing front. 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. <b>NOTE:</b> The thread of the two chassis ground lugs is M5x0.8.	

## Cabling

{This article provides all necessary details to safely connect the platform: connection types, required cables, prerequisites, connection sequences.}

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](#)

## DC power supply inlet

Description	Maximum input current	PSU receptacle model
240 W DC power supply module input connector	7.5 A	Amphenol (Anytek) YK6050423000G

## Preparing the DC power supply cables

<b>NOTICE</b>	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.
<b>WARNING</b>	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.

Kontron suggests the following wire gauges for -48V DC and RTN: 14 AWG or 12 AWG.

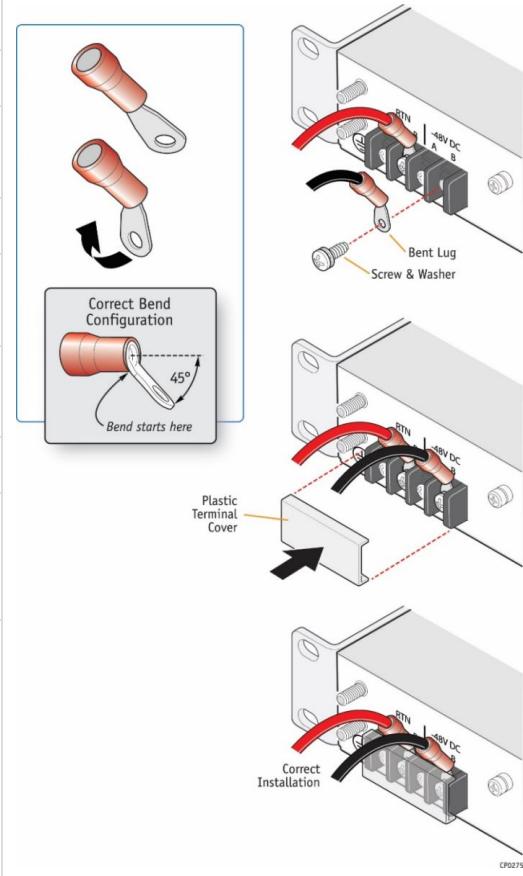
## PRELIMINARY

Description	Quantity	Manufacturer P/N	Link
Crimp lugs: <ul style="list-style-type: none"> <li>Molex insulated spade crimp lugs for 14-16 wire gauge</li> <li>Panduit insulated ring crimp lugs for 10-12 wire gauge</li> </ul>	2 (or 4 for redundancy)	19131-0023 or equivalent	<ul style="list-style-type: none"> <li><a href="#">Molex product catalog</a></li> <li><a href="#">Part details</a></li> </ul>
		EV10-6RB-Q or equivalent	<ul style="list-style-type: none"> <li><a href="#">Panduit product catalog</a></li> <li><a href="#">Part drawing</a></li> </ul>
Black stranded wire to build the power cable based on the length required: <ul style="list-style-type: none"> <li>14 AWG insulation diameter max.: 4.40 mm [ 0.175 in] for Molex crimp lugs</li> <li>12 AWG insulation diameter max.: 5.8 mm [0.23 in] for Panduit crimp lugs</li> </ul>	Length required		
Red stranded wire to build the power cable based on the length required: <ul style="list-style-type: none"> <li>14 AWG insulation diameter max.: 4.40 mm [ 0.175 in] for Molex crimp lug</li> <li>12 AWG insulation diameter max.: 5.8 mm [0.23 in] for Panduit crimp lug</li> </ul>	Length required		
Hand crimp tool: <ul style="list-style-type: none"> <li>Molex Premium Grade Hand Crimp Tool</li> <li>Panduit Hand Crimp Tool</li> </ul>	1	640010100 or equivalent	<ul style="list-style-type: none"> <li><a href="#">Molex product catalog</a></li> <li><a href="#">Application tooling specification sheet</a></li> </ul>
		CT-460 or equivalent	<ul style="list-style-type: none"> <li><a href="#">Panduit product catalog</a></li> <li><a href="#">Application tooling specification sheet</a></li> </ul>

### Procedure

## PRELIMINARY

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	Put the plastic terminal cover back in place once all the cables are screwed in place. <b>NOTE:</b> 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.



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:

## PRELIMINARY

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

Platform end connectors are IEC 320 C13 type female connectors.

Maximum cord length is 2 m.

### AC power supply connection

Step_1	Connect appropriately rated 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](#).

## Software installation and deployment

*{This section provides detailed software installation instructions and the steps required to prepare and to validate the deployment.}*

Children

- [Preparing for installation](#)
- [Installing an operating system on a server](#)
- [Verifying installation](#)
- [Content under creation] Platform installation for high availability
- [Common software installation](#)

## Preparing for installation

*{This article details the steps required to prepare for the installation: obtaining drivers, identifying MAC addresses, selecting a path to install the OS.}*

Step_1	Choose the operating system needed based on the requirements of your application (CentOS 7.4 or latest version is recommended).
Step_2	Confirm the OS version to be installed includes or is compatible with the following network interface drivers: <b>igb</b> and <b>ixgbe</b> .
Step_3	If applicable, download the ISO file of the OS to be installed.

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

For information on components, refer to the [PCI mapping](#).

# Installing an operating system on a server

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

Table of contents

- [Installing an OS on a server using the KVM](#)
  - [Prerequisites](#)
  - [Browser considerations](#)
  - [Connecting to the Web UI of the BMC](#)
  - [Changing the user name and password](#)
  - [Launching the KVM](#)
  - [Mounting the operating system image via virtual media](#)
  - [Accessing the BIOS setup menu](#)
  - [Selecting the boot order from boot override](#)
  - [Completing operating system installation](#)
- [Installing an OS on a server using PXE \(Boot from LAN\)](#)
  - [Completing operating system installation](#)
- [Installing an OS on a server using a USB storage device](#)
  - [Preparing the USB storage device](#)
  - [Configuring Boot Override](#)
  - [Completing operating system installation](#)

The operating system can be installed using the following methods:

- Using the [KVM](#)
- Using [PXE \(Boot from LAN\)](#)
- Using a [USB storage device](#)

## Installing an OS on a server using the KVM

Relevant section:

- [Accessing a BMC on an ME1100](#)

### Prerequisites

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

### Browser considerations

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

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

# PRELIMINARY

Connecting to the Web UI of the BMC

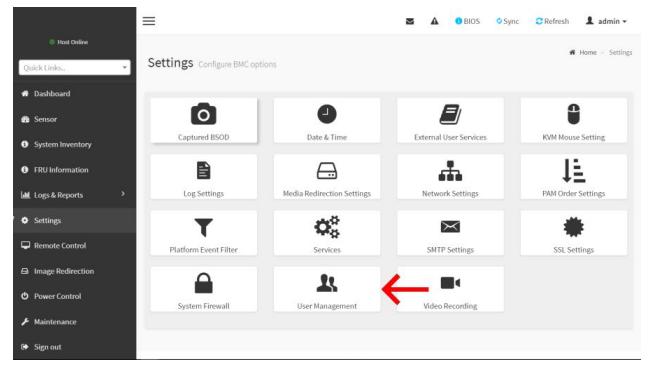
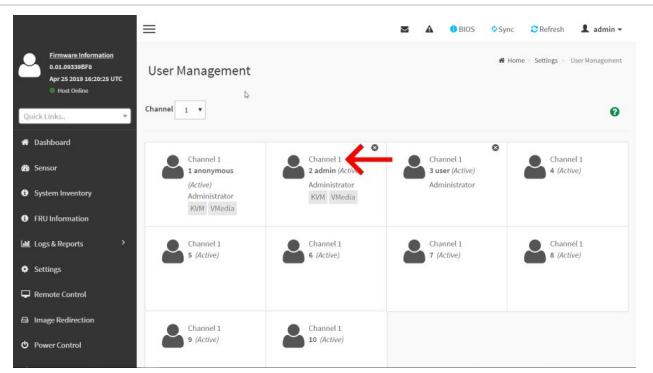
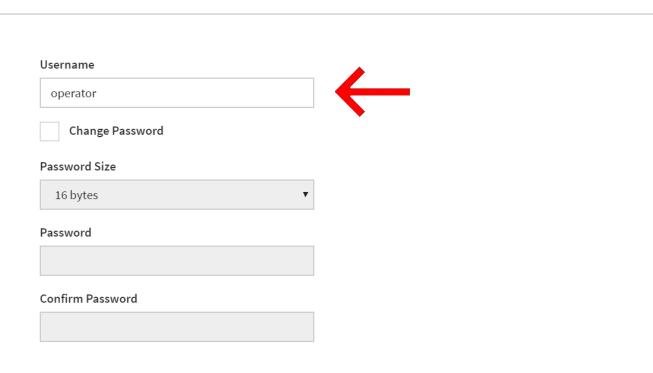
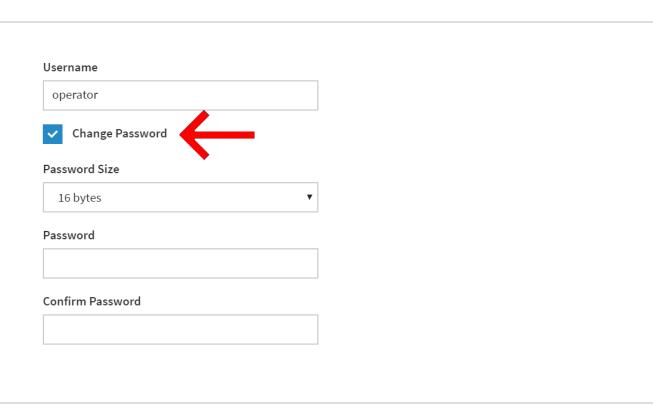
# PRELIMINARY

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

# PRELIMINARY

## Changing the user name and password

**NOTE:** All user names and passwords must have a minimum of 8 characters .

Step_1	<p>Click on <b>Settings</b> in the left side menu and click on <b>User Management</b> .</p> 
Step_2	<p>Select the user to manage.</p> <p><b>NOTE:</b> The first and second users are reserved fields, therefore, their usernames can't be modified.</p> 
Step_3	<p>Change field <b>Username</b> if required.</p> 
Step_4	<p>Check the <b>Change Password</b> box.</p> 
Step_5	<p>Create a new password.</p> 

## PRELIMINARY

Step\_6 Confirm the password.

Username  
operator

Change Password

Password Size  
16 bytes

Password  
.....

Confirm Password  
..... ←

Step\_7 Press **Save**.

Email Format  
AMI-Format

Email ID

Existing SSH Key  
Not Available

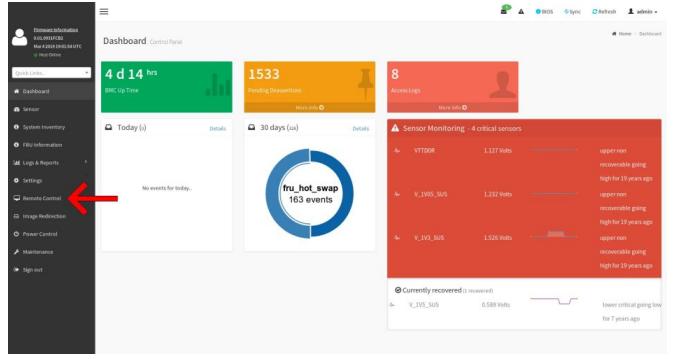
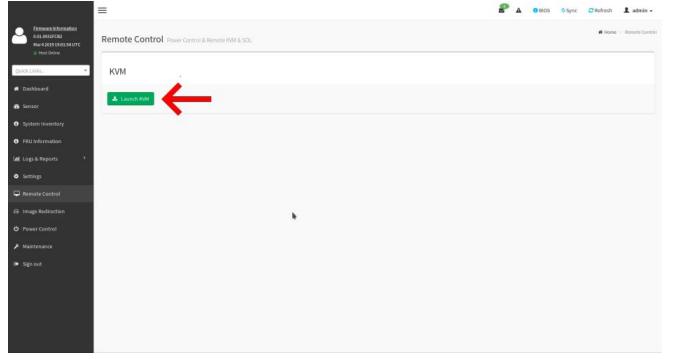
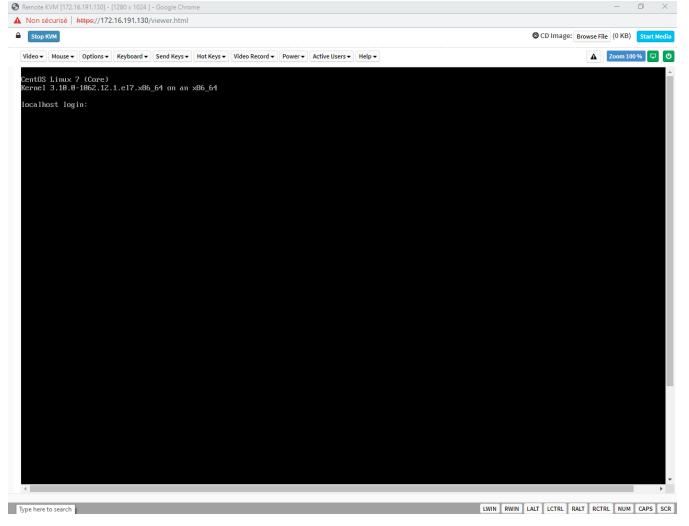
Upload SSH Key  
 →

Delete Save

### Launching the KVM

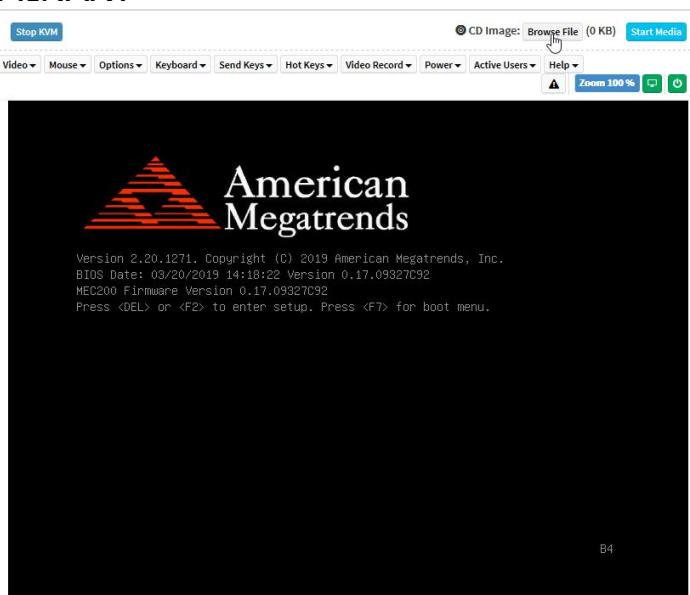
The Web UI allows remote control of the server through a KVM (Keyboard, Video, Mouse) interface.

# PRELIMINARY

<p><b>Step_1</b> From the left menu, click on <b>Remote Control</b>.</p> 	<p><b>Step_2</b> From the <b>Remote Control</b> menu, click on the <b>Launch KVM</b> button.</p> 
<p><b>Step_3</b> A new browser window opens and displays the server screen.  <b>NOTE:</b> If an OS is installed, the image displayed might be that of the OS.</p> 	

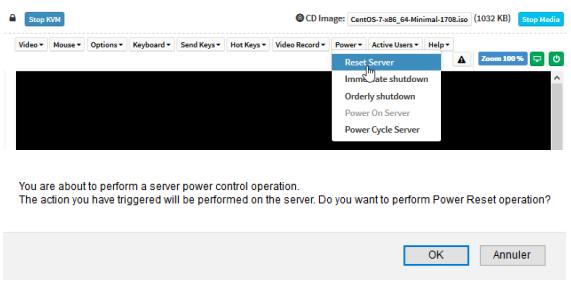
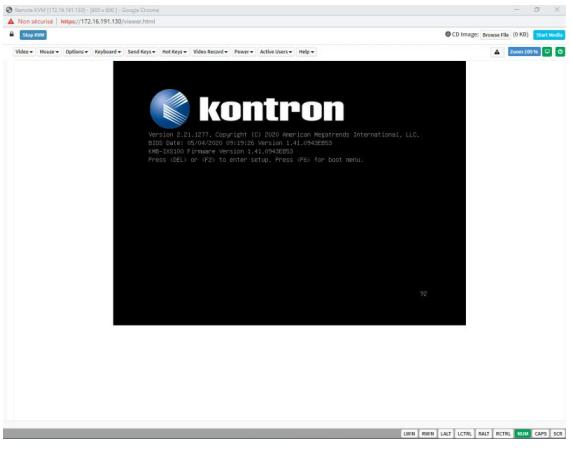
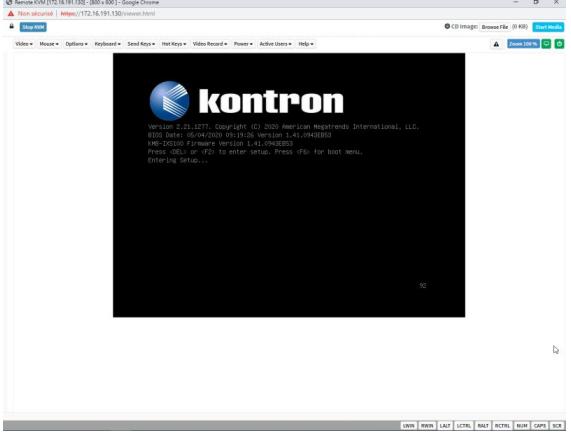
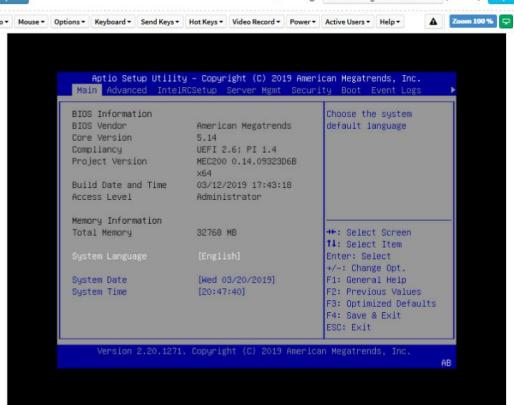
Mounting the operating system image via virtual media

## PRELIMINARY

Step_1	<p>From the KVM view of the server screen, click on <b>Browse File</b> at the top right of the screen. Select the ISO file to be mounted and click on <b>Open</b>.</p>	 <p>The screenshot shows the KVM interface with the American Megatrends logo at the top. Below it, the BIOS version is displayed: Version 2.20.1271, Copyright (C) 2019 American Megatrends, Inc. BIOS Date: 03/20/2019 14:18:22 Version 0.17.09327C92 MEC200 Firmware Version 0.17.09327C92. Instructions to press &lt;DEL&gt; or &lt;F2&gt; to enter setup and &lt;F7&gt; for boot menu.</p>
Step_2	<p>Once the ISO file is loaded, click on <b>Start Media</b> at the top right of the screen. <b>NOTE:</b> Once clicked, the Start Media button becomes the <b>Stop Media</b> button.</p>	 <p>The first screenshot shows the KVM interface with the 'Start Media' button highlighted. The second screenshot shows the same interface after the button has been clicked, now labeled 'Stop Media'.</p>

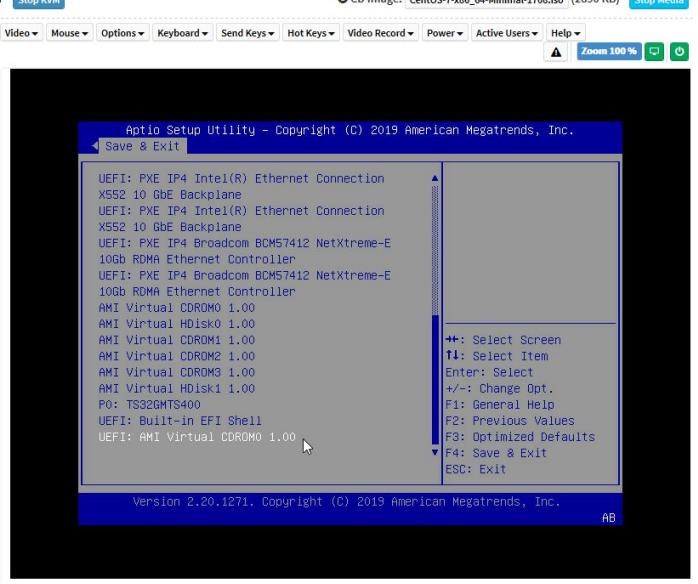
### Accessing the BIOS setup menu

# PRELIMINARY

Step_1	<p>From the <b>Power</b> drop-down menu, select <b>Reset Server</b> to access the BIOS menu. Click on <b>OK</b> to confirm the operation.</p> <p><b>NOTE:</b> When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.</p>	
Step_2	<p>When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.</p> <p><b>NOTE:</b> It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup..."</p> <p><b>Tip:</b> Some users are pressing DEL/F2 many times and very rapidly, to make sure the server catches the key and enters the BIOS setup menu. Doing this may lead to following message on the KVM display: <b>HID Queue is about to get full. Kindly hold on a second(s)..</b> Kontron suggests modifying the <b>Setup Prompt Timeout</b> parameter to give users more time to react. Keeping the focus (single-tasking) on the KVM window is also a good practice to enter the BIOS setup menu each time it is needed.</p> <p>Parameter <b>Setup Prompt Timeout</b> is found in the <b>Boot</b> tab of the BIOS setup menu. The default value is 1 second, but changing it to a value between 3 and 10 seconds is a good target range.</p>	
Step_3	<p>The BIOS sign on screen displays "Entering Setup...".</p> <p><b>NOTE:</b> It will take several seconds to display and enter the BIOS setup menu.</p>	
Step_4	<p>The BIOS setup menu will be displayed.</p>	

# PRELIMINARY

## Selecting the boot order from boot override

Step_1	From the BIOS setup menu and using the keyboard arrows, select the <b>Save &amp; Exit</b> menu. In the <b>Boot Override</b> section, select <b>UEFI: AMI Virtual CDROM0 1.00</b> and press <b>Enter</b> . 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.
--------	--

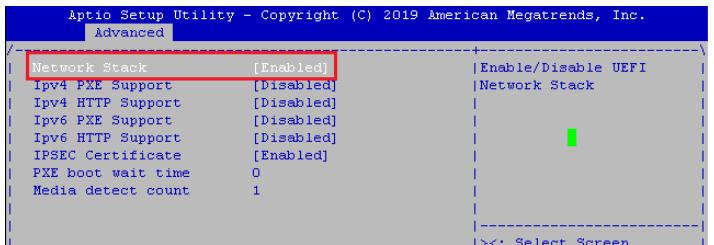
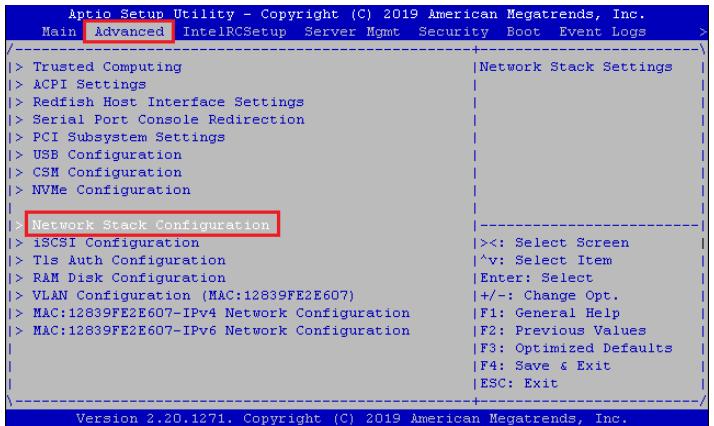
## Installing an OS on a server using PXE (Boot from LAN)

### Relevant section:

- [Accessing the BIOS](#)

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

Step_1	Access the BIOS menu. Refer to Accessing the BIOS.
Step_2	Select the <b>Advanced</b> tab and then the <b>Network Stack Configuration</b> submenu.
Step_3	Enable Network Stack .



# PRELIMINARY

		<p>Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Advanced</p> <table border="0"> <tr><td>Network Stack</td><td>[Enabled]</td><td>[Enabled]</td></tr> <tr><td>IPv4 PXE Support</td><td>[Enabled]</td><td> Enter: Select  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Exit  ESC: Exit</td></tr> <tr><td>IPv4 HTTP Support</td><td>[Disabled]</td><td> ^v: Select Item  +/-.: Change Opt.</td></tr> <tr><td>IPv6 PXE Support</td><td>[Disabled]</td><td> F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Exit  ESC: Exit</td></tr> <tr><td>IPv6 HTTP Support</td><td>[Disabled]</td><td> ^v: Select Item  +/-.: Change Opt.</td></tr> <tr><td>IPSEC Certificate</td><td>[Enabled]</td><td> F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Exit  ESC: Exit</td></tr> <tr><td>PXE boot wait time</td><td>0</td><td> ^v: Select Item  +/-.: Change Opt.</td></tr> <tr><td>Media detect count</td><td>1</td><td> F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Exit  ESC: Exit</td></tr> </table> <p>Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</p>	Network Stack	[Enabled]	[Enabled]	IPv4 PXE Support	[Enabled]	Enter: Select  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit	IPv4 HTTP Support	[Disabled]	^v: Select Item  +/-.: Change Opt.	IPv6 PXE Support	[Disabled]	F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit	IPv6 HTTP Support	[Disabled]	^v: Select Item  +/-.: Change Opt.	IPSEC Certificate	[Enabled]	F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit	PXE boot wait time	0	^v: Select Item  +/-.: Change Opt.	Media detect count	1	F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit
Network Stack	[Enabled]	[Enabled]																								
IPv4 PXE Support	[Enabled]	Enter: Select  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit																								
IPv4 HTTP Support	[Disabled]	^v: Select Item  +/-.: Change Opt.																								
IPv6 PXE Support	[Disabled]	F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit																								
IPv6 HTTP Support	[Disabled]	^v: Select Item  +/-.: Change Opt.																								
IPSEC Certificate	[Enabled]	F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit																								
PXE boot wait time	0	^v: Select Item  +/-.: Change Opt.																								
Media detect count	1	F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit																								
Step_4	Enable IPv4 PXE Support or IPv6 PXE Support, depending on the application.	<p>Aptio Setup - American Megatrends International, LLC.</p> <table border="0"> <tr><td>Security</td><td>Boot</td><td>Save &amp; Exit</td></tr> </table> <p>Restore User Defaults</p> <p>Boot Override</p> <p>CentOS (P4: SAMSUNG MZ7WD480HAGM-00003) UEFI: Patriot Memory PMAP, Partition 1 UEFI: Built-in EFI Shell AMI Virtual CDROM0 1.00 SATA0 P4: SAMSUNG MZ7WD480HAGM SATA0 P5: INTEL SSDSC2KB240GB Generic Ultra HS-SD 1 Patriot Memory PMAP AMI Virtual HDisk0 1.00 Generic Ultra HS-SD 0 UEFI: PXE IP4 American Megatrends Inc. UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 10GBASE-T UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 10GBASE-T</p> <p>++: Select Screen !1: Select Item Enter: Select +/-.: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</p> <p>Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC.</p>	Security	Boot	Save & Exit																					
Security	Boot	Save & Exit																								
Step_5	Reboot the system and access the BIOS setup menu once again.																									
Step_6	Navigate to the Save & Exit menu and then to the Boot Override section.	<p>Aptio Setup - American Megatrends International, LLC.</p> <table border="0"> <tr><td>Security</td><td>Boot</td><td>Save &amp; Exit</td></tr> </table> <p>Restore User Defaults</p> <p>Boot Override</p> <p>CentOS (P4: SAMSUNG MZ7WD480HAGM-00003) UEFI: Patriot Memory PMAP, Partition 1 UEFI: Built-in EFI Shell AMI Virtual CDROM0 1.00 SATA0 P4: SAMSUNG MZ7WD480HAGM SATA0 P5: INTEL SSDSC2KB240GB Generic Ultra HS-SD 1 Patriot Memory PMAP AMI Virtual HDisk0 1.00 Generic Ultra HS-SD 0 UEFI: PXE IP4 American Megatrends Inc. UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 10GBASE-T UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 10GBASE-T</p> <p>++: Select Screen !1: Select Item Enter: Select +/-.: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</p> <p>Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC.</p>	Security	Boot	Save & Exit																					
Security	Boot	Save & Exit																								
Step_7	Choose the PXE option desired.	<p>Aptio Setup - American Megatrends International, LLC.</p> <table border="0"> <tr><td>Security</td><td>Boot</td><td>Save &amp; Exit</td></tr> </table> <p>Restore User Defaults</p> <p>Boot Override</p> <p>CentOS (P4: SAMSUNG MZ7WD480HAGM-00003) UEFI: Patriot Memory PMAP, Partition 1 UEFI: Built-in EFI Shell AMI Virtual CDROM0 1.00 SATA0 P4: SAMSUNG MZ7WD480HAGM SATA0 P5: INTEL SSDSC2KB240GB Generic Ultra HS-SD 1 Patriot Memory PMAP AMI Virtual HDisk0 1.00 Generic Ultra HS-SD 0 UEFI: PXE IP4 American Megatrends Inc. UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 10GBASE-T UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 10GBASE-T</p> <p>++: Select Screen !1: Select Item Enter: Select +/-.: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</p> <p>Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC.</p>	Security	Boot	Save & Exit																					
Security	Boot	Save & Exit																								

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

Completing operating system installation

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

## Installing an OS on a server using a USB storage device

Relevant sections:

- [Accessing the BIOS](#)
- [Platform power management](#)

### Preparing the USB storage device

Step_1	Create a bootable USB key using the appropriate software. NOTE: RUFUS is recommended	
Step_2	Open the USB directory in a remote computer.	
Step_3	Navigate to EFI then BOOT (e.g: E:/EFI/BOOT/).	
Step_4	Open the grub.cfg file with any text editor.	
Step_5	Edit the file and add the following line on the top to activate the serial installation: <i>serial --speed=115200 terminal_input serial terminal_output serial</i>	<pre> 1 serial --speed=115200 2 terminal_input serial 3 terminal_output serial 4 5 set default="1" 6 7 function load_video { 8     insmod efi_gop 9     insmod efi_uga 10    insmod video_bochs 11    insmod video_cirrus 12    insmod all_video 13 } </pre>
Step_6	In the " <i>Test this media &amp; install CentOS 7</i> " entry replace the "quiet" argument with " <i>console=ttyS0,115200n81</i> ".	<pre> 26 ### BEGIN /etc/grub.d/10_linux #### 27 menuentry 'Install CentOS 7' --class fedora --class gnu-linux --class gnu --class os { 28     linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=CENTOS\x207\x20X quiet 29     initrddefi /image/pxeboot/initrd.img 30 } 31 menuentry 'Test this media &amp; install CentOS 7' --class fedora --class gnu-linux --class gnu --class os { 32     linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=CENTOS\x207\x20X rd.live.check quiet console=ttyS0,115200n81 33     initrddefi /images/pxeboot/initrd.img 34 } 35 submenu 'Troubleshooting --&gt;' { 36     menuentry 'Install CentOS 7 in basic graphics mode' --class fedora --class gnu-linux --class gnu --class os { 37         linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=CENTOS\x207\x20X xdriver=vesa nomodeset quiet 38         initrddefi /images/pxeboot/initrd.img 39     } 40     menuentry 'Rescue a CentOS system' --class fedora --class gnu-linux --class gnu --class os { 41         linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=CENTOS\x207\x20X rescue quiet 42         initrddefi /images/pxeboot/initrd.img 43     } 44 } </pre>
Step_7	Save the file and eject the USB key.	

### Configuring Boot Override

# PRELIMINARY

Step_1	Connect the USB storage device on the platform.
Step_2	Power on the platform. Refer to Platform power management.
Step_3	Access the BIOS setup menu. Refer to Accessing the BIOS.
	<p style="font-size: small; margin-top: 5px;">Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</p>
Step_4	Navigate to the <b>Save &amp; Exit</b> menu and then to the <b>Boot Override</b> section.
	<p style="font-size: small; margin-top: 5px;">Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</p>
Step_5	Choose your USB storage device.
	<p><b>NOTE:</b> The USB storage device should be named like this: " <i>UEFI: myUSBname, Partition X</i> ".</p> <p style="font-size: small; margin-top: 5px;">Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</p>

> 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 installation

*{This article details the tests to perform in order to validate that all of the platform's devices are properly mounted and recognized by the OS.}*

## Relevant sections:

[PCI mapping](#)

[Common software installation](#)

	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	<p>Verify that no error messages or warnings are displayed in <b>dmesg</b> using the following commands.</p> <pre>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"</pre> <p><b>NOTE:</b> If there are any messages or warnings displayed, refer to the operating system's documentation to fix them.</p>
Step_3	<p>Verify that the DIMMs are detected.</p> <pre>LocalServer_OSPrompt:~# free -h</pre> <div style="background-color: black; color: white; padding: 5px;"> <pre>[root@localhost ~]# free -h               total        used        free      shared  buff/cache   available Mem:       31G        336M       30G        9.5M     175M       30G Swap:      0B          0B         0B</pre> </div>
Step_4	<p>Verify that all the storage devices are detected.</p> <pre>LocalServer_OSPrompt:~# lsblk</pre> <div style="background-color: black; color: white; padding: 5px;"> <pre>[root@localhost ~]# lsblk NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT sda      8:0    0 29.8G  0 disk └─sda1   8:1    0 200M  0 part /boot       └─sda2   8:2    0 29.6G  0 part                   └─rootvg01-lv01 253:0 0 29.6G 0 lvm  /</pre> </div>
Step_5	<p>Confirm the control plane network interface controller is loaded by the <b>igb</b> driver.</p> <pre>LocalServer_OSPrompt:~# dmesg   grep igb</pre> <p><b>NOTE:</b> You should discover one 1GbE NIC.</p> <div style="background-color: black; color: white; padding: 5px;"> <pre>[root@localhost ~]# dmesg   grep igb [ 4.993339] igb: Intel(R) Gigabit Ethernet Network Driver - version 5.4.0-k [ 5.000268] igb: Copyright (c) 2007-2014 Intel Corporation. [ 5.207811] igb 0000:09:00.0: irq 36 for MSI/MSI-X [ 5.207816] igb 0000:09:00.0: irq 37 for MSI/MSI-X [ 5.207821] igb 0000:09:00.0: irq 38 for MSI/MSI-X [ 5.207825] igb 0000:09:00.0: irq 39 for MSI/MSI-X [ 5.207830] igb 0000:09:00.0: irq 40 for MSI/MSI-X [ 5.237195] igb 0000:09:00.0: added PHC on eth0 [ 5.237195] igb 0000:09:00.0: Intel(R) Gigabit Ethernet Connection [ 5.237197] igb 0000:09:00.0: eth0: (PCIe2.5Gb/s:Width x1) 00:0:a5:d6:33:2c [ 5.237322] igb 0000:09:00.0: eth0: PBA No: 000001-000 [ 5.237323] igb 0000:09:00.0: Using MSI-X interrupts, 4 rx queue(s), 4 tx queue(s) [ 18.287293] igb 0000:09:00.0 eno3: igb: eno3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX</pre> </div>
Step_6	<p>Confirm the data plane network interface controllers are loaded by the <b>ixgbe</b> driver.</p> <pre>LocalServer_OSPrompt:~# dmesg   grep ixgbe</pre> <p><b>NOTE:</b> You should discover two 10GbE NIC.</p> <div style="background-color: black; color: white; padding: 5px;"> <pre>[ 6.516596] ixgbe 0000:04:00.1: MAC: 5, PHY: 14, SFP+: 3, PBA No: 000200-000 [ 6.523639] ixgbe 0000:04:00.1: 00:a0:a5:d6:33:2e [ 6.674120] ixgbe 0000:04:00.1: Intel(R) 10 Gigabit Network Connection [ 13.433172] ixgbe 0000:04:00.0: registered PHC device on eno1 [ 19.225229] ixgbe 0000:04:00.1: registered PHC device on eno2 [ 19.319333] ixgbe 0000:04:00.1 eno2: detected SFP+: 3 [ 19.967523] ixgbe 0000:04:00.1 eno2: NIC Link is Up 10 Gbps, Flow Control: RX/TX</pre> </div>
Step_7	<p>Confirm that all the network interfaces are detected.</p> <pre>LocalServer_OSPrompt:~# ip address</pre> <p><b>NOTE:</b> You should discover one 1GbE NIC and two 10GbE NIC.</p> <div style="background-color: black; color: white; padding: 5px;"> <pre>[root@localhost ~]# ip address 1: lo: &lt;LOOPBACK,UP,LOWER_UP&gt; mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00   inet 127.0.0.1/8 brd 127.0.0.1 scope host lo     valid_lft forever preferred_lft forever   inet6 ::1/128 brd :: scope host     valid_lft forever preferred_lft forever 2: eno3: &lt;BROADCAST,MULTICAST,UP,LOWER_UP&gt; mtu 1500 qdisc mq state UP group default qlen 1000   link/ether 00:a0:a5:d6:33:2d brd ff:ff:ff:ff:ff:ff   inet 172.16.206.11/16 brd 172.16.255.255 scope global noprefixroute dynamic eno3     valid_lft 1208786sec preferred_lft 1208786sec   inet6 fe80::2a0:a5ff:fed6:332d%eno3/64 scope link noprefixroute     valid_lft forever preferred_lft forever 3: eno1: &lt;NO-CARRIER,BROADCAST,MULTICAST,UP&gt; mtu 1500 qdisc mq state DOWN group default qlen 1000   link/ether 00:a0:a5:d6:33:2e brd ff:ff:ff:ff:ff:ff 4: eno2: &lt;BROADCAST,MULTICAST,UP,LOWER_UP&gt; mtu 1500 qdisc mq state UP group default qlen 1000   link/ether 00:a0:a5:d6:33:2e brd ff:ff:ff:ff:ff:ff   inet6 fe80::2a0:a5ff:fed6:332e%eno2/64 scope link     valid_lft forever preferred_lft forever</pre> </div>

## PRELIMINARY

```
valid_lft forever preferred_lft forever
5: eno2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:a5:d6:33:2e brd ff:ff:ff:ff:ff:ff
    inet 6 fe80::2a0:a5ff:fed:332e/64 scope link
        valid_lft forever preferred_lft forever
```

Step_8	<p>Configure network interface controllers based on your requirements.</p> <p><b>NOTE:</b> 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.</p>	<p><b>Control plane</b></p> <p><b>Data plane</b></p> <p><b>Network controller</b></p>
Step_9	<p>Install ipmitool and pciutils using the package manager, and update the operating system packages. The ipmitool version recommended is 1.8.18.</p> <p>Example:</p> <pre>LocalServer_OSPrompt:~# yum update LocalServer_OSPrompt:~# yum install ipmitool LocalServer_OSPrompt:~# yum install pciutils</pre> <p><b>NOTE:</b> Updating the packages may take a few minutes.</p>	
Step_10	<p>(Optional) If a PCIe add-in card is installed, verify that the card is detected.</p> <pre>LocalServer_OSPrompt:~# lspci</pre>	<pre>[root@localhost ~]# lspci [ 00:00.0 Host bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DMi2 (rev 03) [ 00:01.0 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 1 (rev 03) [ 00:01.1 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 1 (rev 03) [ 00:02.0 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 2 (rev 03) [ 00:02.2 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 2 (rev 03) [ 00:03.0 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 3 (rev 03) [ 00:03.9 System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Host Plug (rev 03) [ 00:05.0 System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO RAS/Control Status/Global Errors (rev 03) [ 00:05.4 PIC: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D I/O APIC (rev 03) [ 00:16.0 Communication controller: Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller #1 (rev 04) [ 00:16.1 Communication controller: Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller #2 (rev 04) [ 00:1c.0 PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #1 (rev d5) [ 00:1c.4 PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #5 (rev d5) [ 00:1d.0 USB controller: Intel Corporation 8 Series/C220 Series Chipset Family USB EHCI #1 (rev 05) [ 00:1d.1 ISA bridge: Intel Corporation C224 Series Chipset Family Server Standard SKO LPC Controller (rev 05) [ 00:1f.2 SATA controller: Intel Corporation 8 Series/C220 Series Chipset Family 6-port SATA Controller 1 [AHCI mode] (rev 05) [ 00:1f.3 SMBus: Intel Corporation 8 Series/C220 Series Chipset Family SMBus Controller (rev 05)</pre>
Step_11	<p>Verify communication between the operating system and the BMC.</p> <pre>LocalServer_OSPrompt:~# ipmitool mc info</pre>	<pre>LocalServer_OSPrompt:~# ipmitool mc info Device ID          : 32 Device Revision    : 1 Firmware Revision  : 0.01 IPMI Version       : 2.0 Manufacturer ID    : 15000 Manufacturer Name  : Kontron Product ID         : 1100 (0x044c) Product Name        : Unknown (0x44c) Device Available   : yes Provides Device SDRs: no Additional Device Support:   Sensor Device   SDR Repository Device   SEL Device   FRU Inventory Device   IPMB Event Receiver   IPMB Event Generator   Chassis Device Aux Firmware Rev Info   0x09   0x33   0x9b   0xf8</pre>

## Common software installation

*{This article provides a list of required and recommended software tools for platform configuration, operation and troubleshooting.}*

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

Tool	Description	Installation
ipmitool	IPMI utility for controlling and monitoring the devices through the IPMI interfaces of the platform.	From a command prompt: LocalServer_OSPrompt# <b>sudo apt install ipmitool</b>
pciutils	Tool used to manage PCIe cards connected to the platform.	From a command prompt: LocalServer_OSPrompt# <b>sudo apt install pciutils</b>
snmp	Net-SNMP default package.	From a command prompt: RemoteComputer_OSPrompt:~# <b>yum install snmp</b>
snmp-mibs-downloader	Tool used to install and manage MIB (Management Information Base) files.	From a command prompt: RemoteComputer_OSPrompt:~# <b>yum install snmp-mibs-downloader</b>

## Recommended software tools

Tool	Description	Installation
PuTTY	Serial console tool recommended in the documentation.	Refer to PuTTY's documentation.
jq	Command-line tool used to parse raw JSON data to make the Redfish API response human-readable.	From a command prompt: RemoteComputer_OSPrompt:~# <b>sudo apt install jq</b>
cURL	HTTP/FTP client tool used to navigate the Web API using a command-line tool.	From a command prompt: RemoteComputer_OSPrompt:~# <b>sudo apt install curl</b>
JSON viewer browser add-on	If the Redfish API is used through an Internet browser, a JSON viewer is recommended to make the output human-readable.	Refer to the browser's documentation.

## Configuring

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

Children

- [Configuring system access methods](#)
- [Configuring and managing users](#)
- [Baseboard management controller - BMC](#)
- [Configuring the network time protocol - NTP](#)
- [Basic BIOS option configuration](#)
- [Content under creation] Network infrastructure integration
- [Content under creation] Parallel configuration
- [Content under creation] High availability

# Configuring system access methods

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

Table of contents

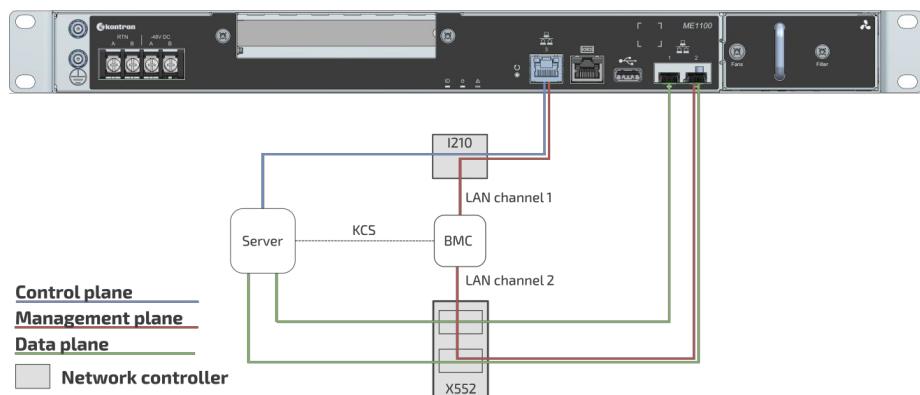
- [General considerations and warnings about network configuration](#)
- [Disabling IOL on a LAN channel](#)
  - [Disabling IOL on a LAN channel using IPMI](#)
- [Enabling IOL on a LAN channel](#)
  - [Enabling IOL on a LAN channel using IPMI](#)
- [Configuring Serial over LAN parameters using IPMI](#)
  - [Accessing the BMC](#)
  - [Viewing and configuring SOL parameters](#)
- [Creating the Redfish root URL](#)
  - [Prerequisites](#)
  - [Procedure](#)
- [Configuring BMC SNMP](#)
  - [Enabling SNMP for a user using the BMC Web UI](#)
  - [Installing SNMP on a server](#)
  - [Verifying SNMP communication for a user](#)
  - [Disabling an SNMP access](#)

## General considerations and warnings about network configuration

The architecture of the ME1100 platform offers many entry points, including two LAN channels to the BMC.

**Use caution when configuring network accesses. Your access to the system could be interrupted should you disable the access point you entered through.**

As an example, if BMC LAN channel 2 is disabled and you access BMC LAN channel 1 through IOL to disable IOL on LAN channel 1, your connection will be interrupted and you will essentially have locked yourself out of the BMC as both LAN channels will now be disabled.



## Disabling IOL on a LAN channel

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

On a LAN channel, IOL can be disabled:

- Using [IPMI](#)

**NOTE:** It is currently not possible to disable a LAN channel using the BIOS setup menu.

### Disabling IOL on a LAN channel using IPMI

# PRELIMINARY

## Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to [Accessing a BMC on an ME module using IPMI \(KCS\)](#).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#).

The following procedures will be executed using the [Accessing a BMC on an ME module using IPMI \(KCS\)](#) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT\_IP] -U [IPMI user name] -P [IPMI password].

## Disabling IOL on a LAN channel

NOTE: LAN channel 1 corresponds to the RJ45 connector (port 3) and LAN channel 2 corresponds to the SFP connector (port 2).

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

## Enabling IOL on a LAN channel

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

On a LAN channel, IOL can be enabled:

- Using [IPMI](#)

NOTE: It is currently not possible to enable a LAN channel using the BIOS setup menu.

## Enabling IOL on a LAN channel using IPMI

### Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to [Accessing a BMC on an ME module using IPMI \(KCS\)](#).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#).

The following procedures will be executed using the [Accessing a BMC on an ME module using IPMI \(KCS\)](#) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT\_IP] -U [IPMI user name] -P [IPMI password].

## Enabling IOL on a LAN channel

NOTE: LAN channel 1 corresponds to the RJ45 connector (port 3) and LAN channel 2 corresponds to the SFP connector (port 2).

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

## Configuring Serial over LAN parameters using IPMI

# PRELIMINARY

## Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to [Accessing a BMC on an ME module using IPMI \(KCS\)](#).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#).

The following procedures will be executed using the [Accessing a BMC on an ME module using IPMI \(KCS\)](#) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT\_IP] -U [IPMI user name] -P [IPMI password].

## Viewing and configuring SOL parameters

Step_1	Display SOL parameters. LocalServer_OSPrompt:~# ipmitool sol info	\$ ipmitool sol info Set in progress : set-complete Enabled : true Force Encryption : false Force Authentication : false Privilege Level : ADMINISTRATOR Character Accumulate Level (ms) : 60 Character Send Threshold : 96 Retry Count : 7 Retry Interval (ms) : 500 Volatile Bit Rate (kbps) : 115.2 Non-Volatile Bit Rate (kbps) : 115.2 Payload Channel : 1 (0x01) Payload Port : 623
Step_2	Display SOL parameters available for configuration. LocalServer_OSPrompt:~# ipmitool sol set	\$ ipmitool sol set SOL set parameters and values: set-in-progress set-complete   set-in-progress   commit-write enabled true   false force-encryption true   false force-authentication true   false privilege-level user   operator   admin   oem character-accumulate-level <in 5 ms increments> character-send-threshold N retry-count N retry-interval <in 10 ms increments> non-volatile-bit-rate serial   9.6   19.2   38.4   57.6   115.2 volatile-bit-rate serial   9.6   19.2   38.4   57.6   115.2
Step_3	Set the desired parameters. LocalServer_OSPrompt:~# ipmitool sol set [PARAMETER] [PARAMETER_VALUE] [LAN_CHANNEL]	\$ ipmitool sol set non-volatile-bit-rate 115.2 1

## Creating the Redfish root URL

### Prerequisites

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

### Relevant sections:

[Baseboard management controller - BMC](#)

[Common software installation](#)

[Default user names and passwords](#)

### Procedure

## PRELIMINARY

Step_1	Begin URL with the <b>https</b> prefix.	<b>https://</b>
Step_2	Add the Redfish username and password separated by a colon.	<b><a href="https://Administrator:superuser">https://Administrator:superuser</a></b>
Step_3	Add @ to the URL followed by the BMC management IP address.	<b><a href="https://Administrator:superuser@172.16.205.245">https://Administrator:superuser@172.16.205.245</a></b>
Step_4	Add the Redfish API suffix to the URL.	<b><a href="https://Administrator:superuser@172.16.205.245/redfish/v1/">https://Administrator:superuser@172.16.205.245/redfish/v1/</a></b>
Step_5	Access the API using an HTTP client and verify that the URL is valid.	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/ {"@odata.context":"/redfish/v1/\$metadata#ServiceRoot.ServiceRoot","@odata.etag": "W/\"1563368478\"","@odata.id":"/redfish/v1/","@odata.type":"#ServiceRoot.v1_2_0 .ServiceRoot","AccountService":{"@odata.id":"/redfish/v1/AccountService"},"Chass is":{"@odata.id":"/redfish/v1/Chassis"},"CompositionService":{"@odata.id":"/redf ish/v1/CompositionService"},"Description":"The service root for all Redfish requ ests on this host","EventService":{"@odata.id":"/redfish/v1/EventService"},"Id": "RootService","JsonSchemas":[{"@odata.id":"/redfish/v1/JsonSchemas"}],"Links":{" Sessions":[{"@odata.id":"/redfish/v1/SessionService/Sessions"}]}, "Managers":{@odata .id":"/redfish/v1/Managers"}, "Name": "Root Service", "Oem": {"Ami": {"@odata.type": "AMIServiceRoot.v1_0_0.AMIServiceRoot"}, "Configurations": {"@odata.id":"/redfish/v1 /configurations"}, "RtpVersion": "1.2.1"}, "Dre": {"@odata.type": "#AMIDynamicExtensi on.v1_0_0.AMIDynamicExtension"}, "DynamicExtension": {"@odata.id":"/redfish/v1/Dyna micExtension"}}, "RedfishVersion": "1.2.1", "Registries": {"@odata.id":"/redfish/v1/Regis tries"}, "SessionService": {"@odata.id":"/redfish/v1/SessionService"}, "Syste ms": {"@odata.id":"/redfish/v1/Systems"}, "Tasks": {"@odata.id":"/redfish/v1/TaskSe rvice"}, "TelemetryService": {"@odata.id":"/redfish/v1/TelemetryService"}, "UUID": " 00a0a5d6-332a-c503-0010-debfa0af8f6b", "UpdateService": {"@odata.id":"/redfish/v1/ UpdateService"}}</pre>

## Configuring BMC SNMP



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

**NOTE :** The current implementation supports version 3 of the SNMP protocol. For the commands to work, snmpwalk version 5.8 or higher must be installed.

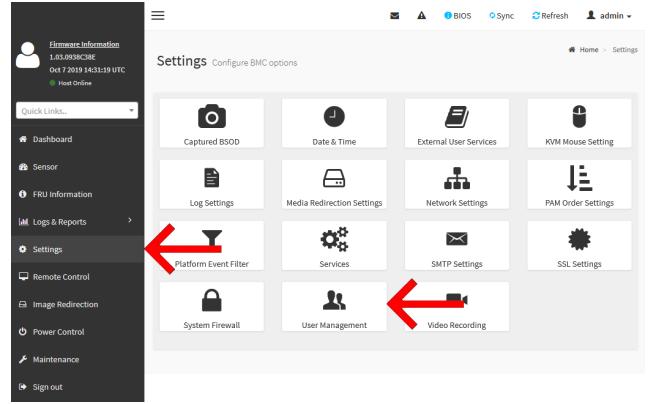
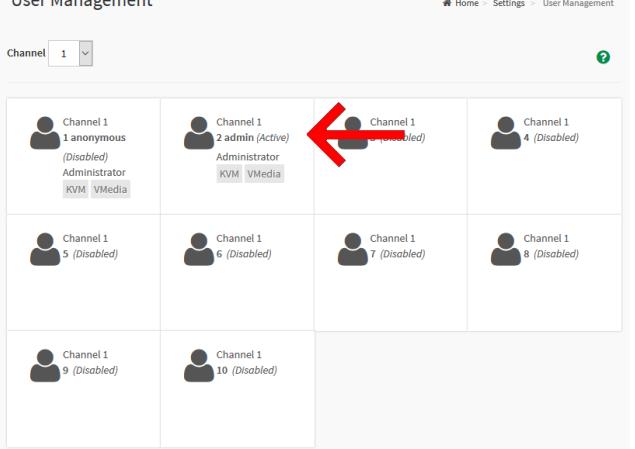
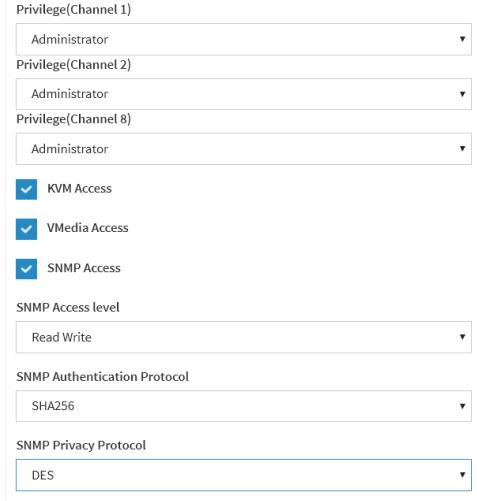
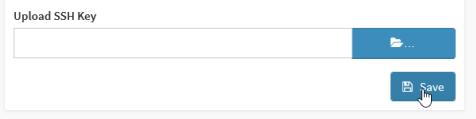
### Enabling SNMP for a user using the BMC Web UI

Relevant section:

[Configuring and managing users](#)

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

# PRELIMINARY

Step_1	<p>From the left menu, click on <b>Settings</b> and then <b>User Management</b>.</p>	
Step_2	Select the user.	
Step_3	Click on the <b>SNMP Access</b> checkbox to give the user an SNMP access.	
Step_4	Choose the <b>SNMP Access Level</b> . <b>NOTE :</b> Once SNMP access is enabled, the password's minimal security increases, a minimum of 8 characters will be required.	
Step_5	Choose the <b>SNMP Authentication Protocol</b> .	
Step_6	Choose the <b>SNMP Privacy Protocol</b> .	
Step_7	Click on <b>Save</b> .	

## Installing SNMP on a server

**NOTE:** The package manager may vary depending on the OS installed.

Step_1	<p>From a remote computer that has access to the management network subnet , install SNMP. RemoteComputer_OSPrompt:~# <b>yum install snmp</b></p>
Step_2	<p>(Optional) To be able to see human-readable MIBs (instead of seeing the OID), also install snmp-mibs-downloader. RemoteComputer_OSPrompt:~# <b>yum install snmp-mibs-downloader</b></p>

# PRELIMINARY

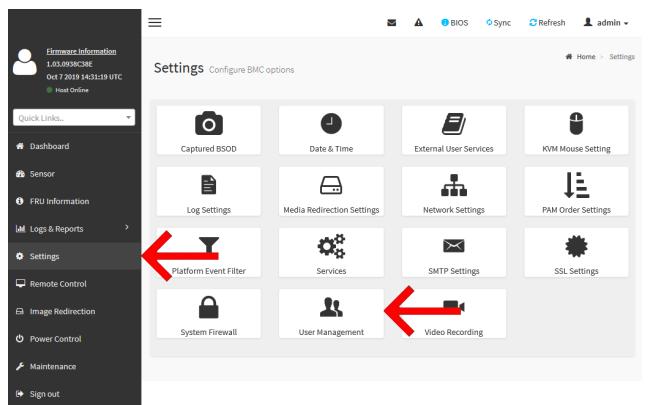
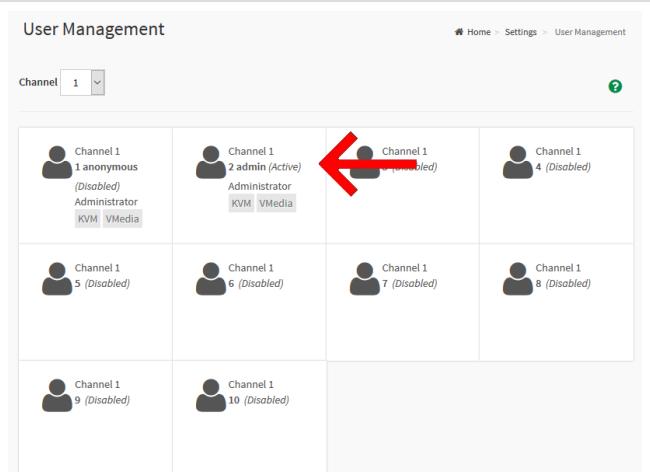
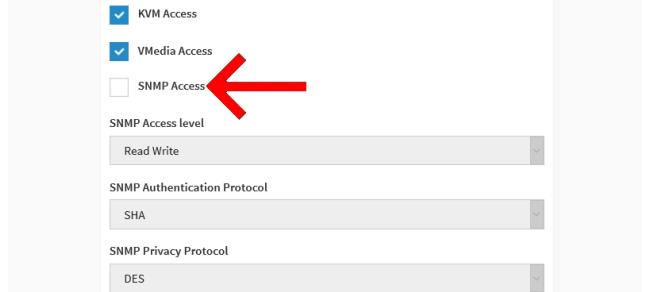
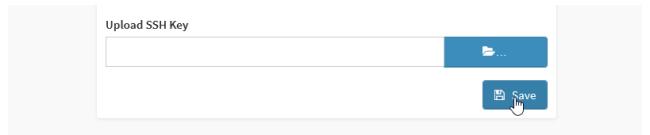
## Verifying SNMP communication for a user

Step_1	<p>From a remote computer that has access to the management network subnet, verify that the BMC properly responds to the SNMP request.</p> <p>RemoteComputer_OSPrompt:~# snmpwalk -v 3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [SNMP_PASSWORD] -x [PRIVACY_PROTOCOL] -X [SNMP_PASSWORD] [BMC MNGMT_IP]</p> <pre>Snmpwalk -v 3 -l authPriv -u snmpaccess -a SHA-256 -A snmppassword -x DES -X snmppassword 172.16.192.250 SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSmagentOIDs.10 SNMPv2-MIB::sysContact.0 = STRING: root@kontron-eth0 SNMPv2-MIB::sysName.0 = STRING: ME1100_00AABAD5D3E90 SNMPv2-MIB::sysUpTime.0 = Timeticks: (56360) 0:09:25.60 SNMPv2-MIB::sysLastChange.0 = Timeticks: (14) 0:00:08.14 SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpfameoverKMBCompliance SNMPv2-MIB::sysORID.2 = OID: SNMP-FRAMEWORK-MIB::snmpfameoverKMBCompliance SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMNCCompliance SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::tcpMIB SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB SNMPv2-MIB::sysORID.6 = OID: UDP-MIB::udpMIB SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance SNMPv2-MIB::sysORID.10 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB. SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching. SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing implementations for the SNMP User-based Security Model. SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities. SNMPv2-MIB::sysORDescr.5 = STRING: View-based Access Control Model for SNMP SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP Implementations SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing IP and ICMP Implementations SNMPv2-MIB::sysORDescr.8 = STRING: The MIB module for managing UDP Implementations SNMPv2-MIB::sysORDescr.9 = STRING: The MIB module for managing SNMP Notifications, plus filtering. SNMPv2-MIB::sysORUptime.1 = Timeticks: (4) 0:00:00.04 SNMPv2-MIB::sysORUptime.2 = Timeticks: (5) 0:00:00.05 SNMPv2-MIB::sysORUptime.3 = Timeticks: (5) 0:00:00.05 SNMPv2-MIB::sysORUptime.4 = Timeticks: (5) 0:00:00.05 SNMPv2-MIB::sysORUptime.5 = Timeticks: (7) 0:00:00.07 SNMPv2-MIB::sysORUptime.6 = Timeticks: (7) 0:00:00.07 SNMPv2-MIB::sysORUptime.7 = Timeticks: (7) 0:00:00.07 SNMPv2-MIB::sysORUptime.8 = Timeticks: (14) 0:00:00.14 SNMPv2-MIB::sysORUptime.9 = Timeticks: (14) 0:00:00.14 IF-MIB::ifIndex.0 = INTEGER: 0 IF-MIB::ifIndex.1 = INTEGER: 1 IF-MIB::ifIndex.2 = INTEGER: 2 IF-MIB::ifIndex.3 = INTEGER: 3 IF-MIB::ifIndex.4 = INTEGER: 4 IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifIndex.6 = INTEGER: 6 IF-MIB::ifDescr.1 = STRING: lo IF-MIB::ifDescr.2 = STRING: eth0 IF-MIB::ifDescr.3 = STRING: eth1</pre>
--------	---

## Disabling an SNMP access

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

# PRELIMINARY

<p><b>Step_1</b> Access the BMC Web UI.</p>	
<p><b>Step_2</b> From the left menu, click on <b>Settings</b> and then <b>User Management</b>.</p> 	
<p><b>Step_3</b> Select the user.</p>	
<p><b>Step_4</b> Click on the <b>SNMP Access</b> checkbox to disable the SNMP access of the user selected.</p>	
<p><b>Step_5</b> Click on <b>Save</b> .</p>	

# Configuring and managing users

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

Table of contents

- [Configuring BMC users](#)
  - [Configuring BMC user names and passwords](#)
  - [Adding a BMC user](#)
  - [Deleting or disabling a BMC user](#)
  - [Configuring privilege level for BMC users](#)
- [Managing Redfish users](#)
  - [Configuring Redfish user names and passwords](#)
  - [Adding a Redfish user](#)
  - [Deleting a Redfish user](#)
  - [Configuring Redfish privilege level](#)
- [Configuring SNMP users using BMC SNMP](#)
- [Configuring OS users](#)

## Configuring BMC users

	Administrator rights are required to manage users.
---	--

### Configuring BMC user names and passwords

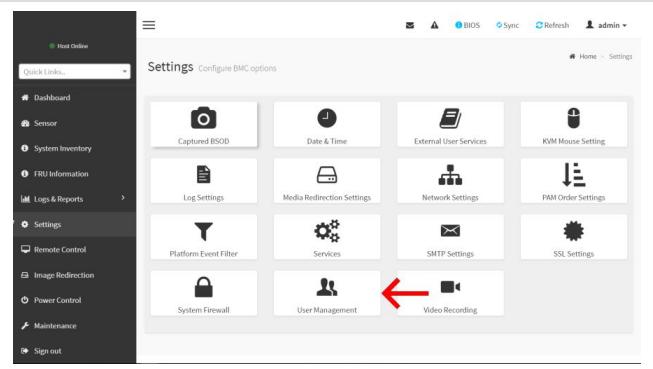
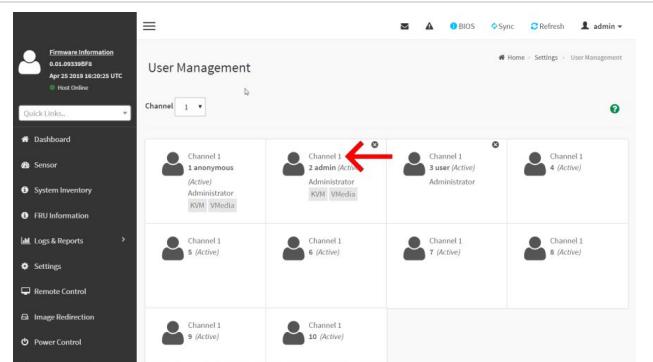
For default user names and passwords, refer to [Default user names and passwords](#).

BMC user names and passwords can be managed:

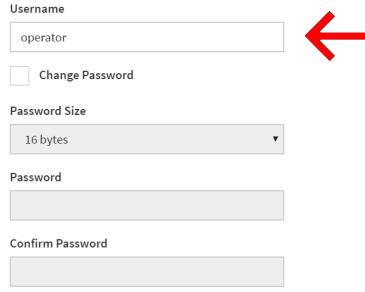
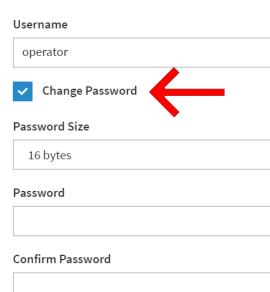
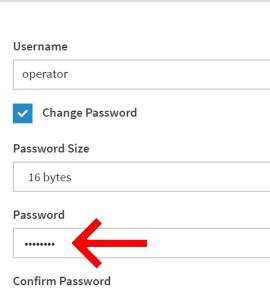
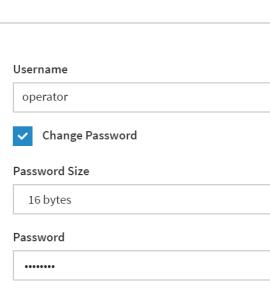
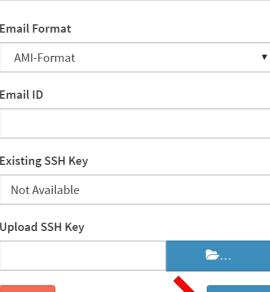
- Using the [Web UI](#)
- Using [IPMI over LAN \(IOL\)](#)
- Using [IPMI via KCS](#)

### Configuring BMC user names and passwords using the Web UI

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

Step_1	<p>Click on <b>Settings</b> in the left side menu and click on <b>User Management</b>.</p> 
Step_2	<p>Select the user to manage.</p> <p><b>NOTE:</b> The first and second users are reserved fields, therefore, their usernames can't be modified.</p> 

## PRELIMINARY

Step_3	Change field <b>Username</b> if required.	
Step_4	Check the <b>Change Password</b> box.	
Step_5	Create a new password.	
Step_6	Confirm the password.	
Step_7	Press <b>Save</b> .	

Configuring BMC user names and passwords using IPMI over LAN (IOL)

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

# PRELIMINARY

Step_1	<p>From a remote computer that has access to the management network subnet, print the BMC user list.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin user list ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2      admin       false  false   true    ADMINISTRATOR 3     operator     true   false  false    ADMINISTRATOR 4              true  false  false    NO ACCESS 5              true  false  false    NO ACCESS 6              true  false  false    NO ACCESS 7              true  false  false    NO ACCESS 8              true  false  false    NO ACCESS 9              true  false  false    NO ACCESS 10             true  false  false    NO ACCESS</pre>
Step_2	Identify the ID number of the user to be changed.	<pre>[root@localhost ~]# ipmitool -H 192.168.101.26 -U admin -P admin user list ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2      admin       false  false   true    ADMINISTRATOR 3     user        true   false  false    ADMINISTRATOR 4              true  false  false    NO ACCESS 5              true  false  false    NO ACCESS 6              true  false  false    NO ACCESS 7              true  false  false    NO ACCESS 8              true  false  false    NO ACCESS 9              true  false  false    NO ACCESS 10             true  false  false    NO ACCESS</pre>
Step_3	<p>Change the user name.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user set name [IPMI user ID] [new IPMI user name]</pre> <p>NOTE: The first and second user names of the user list are reserved fields and therefore can't be modified.</p>	
Step_4	<p>Verify that the user name has been updated correctly by printing the user list.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin user list ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2      admin       false  false   true    ADMINISTRATOR 3     operator     true   false  false    ADMINISTRATOR 4              true  false  false    NO ACCESS 5              true  false  false    NO ACCESS 6              true  false  false    NO ACCESS 7              true  false  false    NO ACCESS 8              true  false  false    NO ACCESS 9              true  false  false    NO ACCESS 10             true  false  false    NO ACCESS</pre>
Step_5	<p>Change the password.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user set password [IPMI user ID] [new IPMI password]</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin user set password 3 newpassword Set User Password command successful (user 3)</pre>
Step_6	<p>Enable the user.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool user enable [ IPMI user ID ]</pre>	
Step_7	<p>Configure privilege level.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]</pre>	
Step_8	<p>Verify that credentials updated correctly by using any ipmitool command.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [new IPMI user name] -P [new IPMI password] [IPMI command]</pre> <p>NOTE: Other parameters could limit the accessibility of the user that is trying to manage the BMC. Refer to ipmitool documentation for further information.</p>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U operator -P newpassword user list ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2      admin       false  false   true    ADMINISTRATOR 3     operator     true   false  false    ADMINISTRATOR 4              true  false  false    NO ACCESS 5              true  false  false    NO ACCESS 6              true  false  false    NO ACCESS 7              true  false  false    NO ACCESS 8              true  false  false    NO ACCESS 9              true  false  false    NO ACCESS 10             true  false  false    NO ACCESS</pre>

## Configuring BMC user names and passwords using IPMI via KCS

# PRELIMINARY

Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

Step_1	<p>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, print the BMC user list.</p> <pre>LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]</pre>	<pre>[root@localhost ~]# ipmitool user list 1 ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2 admin         false  false   true    ADMINISTRATOR 3 user          true   true   true    ADMINISTRATOR 4              true  false   false   NO ACCESS 5              true  false   false   NO ACCESS 6              true  false   false   NO ACCESS 7              true  false   false   NO ACCESS 8              true  false   false   NO ACCESS 9              true  false   false   NO ACCESS 10             true  false   false   NO ACCESS</pre>
Step_2	<p>Identify the ID number of the user to be changed.</p>	<pre>[root@localhost ~]# ipmitool user list 1 ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2 admin         false  false   true    ADMINISTRATOR 3 user          true   true   true    ADMINISTRATOR 4              true  false   false   NO ACCESS 5              true  false   false   NO ACCESS 6              true  false   false   NO ACCESS 7              true  false   false   NO ACCESS 8              true  false   false   NO ACCESS 9              true  false   false   NO ACCESS 10             true  false   false   NO ACCESS</pre>
Step_3	<p>Change the user name.</p> <pre>LocalServer_OSPrompt: ~# ipmitool user set name [IPMI user ID] [new IPMI user name]</pre> <p><b>NOTE:</b> The first and second user names of the user list are reserved fields and therefore can't be modified.</p>	
Step_4	<p>Verify that the user name has updated correctly by printing the user list.</p> <pre>LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]</pre>	<pre>[root@localhost ~]# ipmitool user list 1 ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2 admin         false  false   true    ADMINISTRATOR 3 operator      true   true   true    ADMINISTRATOR 4              true  false   false   NO ACCESS 5              true  false   false   NO ACCESS 6              true  false   false   NO ACCESS 7              true  false   false   NO ACCESS 8              true  false   false   NO ACCESS 9              true  false   false   NO ACCESS 10             true  false   false   NO ACCESS</pre>
Step_5	<p>Change the password.</p> <pre>LocalServer_OSPrompt: ~# ipmitool user set password [IPMI user ID] [new IPMI password]</pre>	<pre>[root@localhost ~]# ipmitool user set password 3 newpassword Set User Password command successful (user 3)</pre>
Step_6	<p>Verify that the credentials updated correctly by using an access method that requires a login.</p> <p><b>NOTE:</b> Other parameters could limit the accessibility of the user that is trying to manage the BMC. Refer to ipmitool documentation.</p>	

## Adding a BMC user

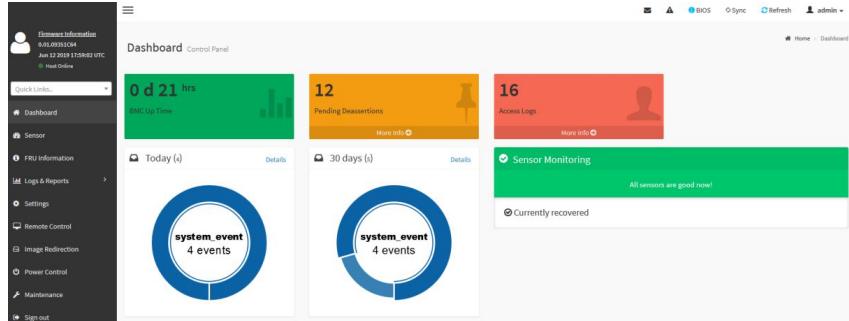
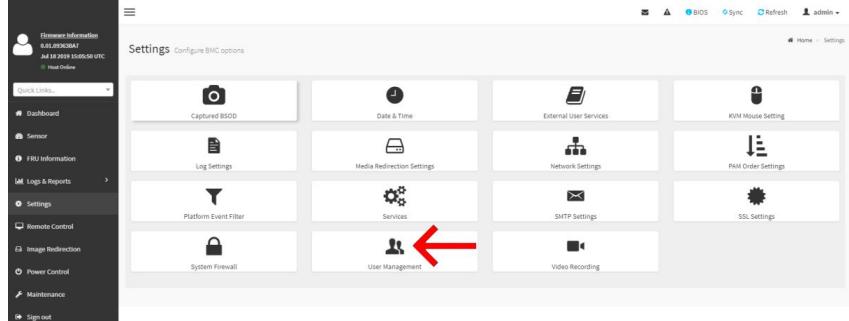
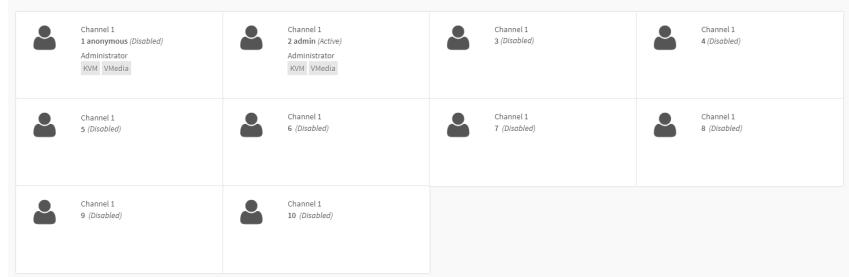
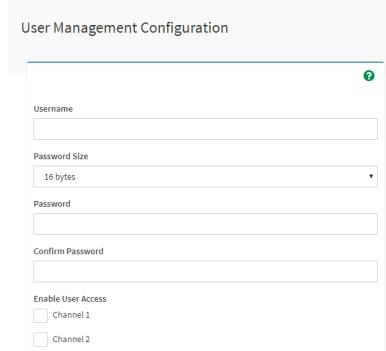
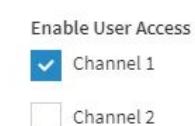
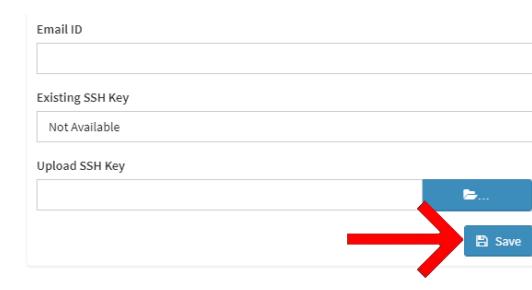
BMC users can be added :

- Using the [Web UI](#)
- Using [IPMI over LAN \(IOL\)](#)
- Using [IPMI via KCS](#)

## Adding a BMC user using the Web UI

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

# PRELIMINARY

Step_1	Access the BMC Web UI of the server.	 <p>The screenshot shows the BMC Web UI dashboard. On the left, there's a sidebar with navigation links like Dashboard, Sensor, FRU Information, Logs &amp; Reports, Settings, Remote Control, Image Redirection, Power Control, Maintenance, and Sign out. The main area displays a summary of system health: 0 days 21 hours since last boot, 12 pending decomissions, 16 access logs, and two circular event monitors for today and 30 days, both showing 4 events each. A green banner at the bottom right says "All sensors are good now! Currently recovered".</p>
Step_2	Click on <b>Settings</b> in the left side menu and click on <b>User Management</b> .	 <p>The screenshot shows the BMC Web UI settings page. The left sidebar has the same navigation as the dashboard. The main area is titled "Settings Configure BMC options" and contains a grid of icons for various configuration options: Captured ISO, Date &amp; Time, External User Services, IPMI Mouse Setting, Log Settings, Media Redirection Settings, Network Settings, Platform Event Filter, Services, SMTP Settings, System Firewall, and User Management. A red arrow points to the "User Management" icon.</p>
Step_3	<p>Select the ID of the user to enable .</p> <p><b>NOTE:</b> The first and second users are reserved fields and therefore can't be modified.</p>	 <p>The screenshot shows a list of users in the BMC Web UI. There are two rows of four users each. The columns are labeled with Channel numbers and their status: Channel 1 (1 anonymous (Disabled), Administrator KVM / VMedia), Channel 2 (2 admin (Active), Administrator KVM / VMedia), Channel 3 (3 (Disabled)), Channel 4 (4 (Disabled)), Channel 5 (5 (Disabled)), Channel 6 (6 (Disabled)), Channel 7 (7 (Disabled)), Channel 8 (8 (Disabled)), Channel 9 (9 (Disabled)), and Channel 10 (10 (Disabled)).</p>
Step_4	<p>Configure the user according to the application's requirements.</p> <p><b>NOTE:</b> Refer to <a href="#">Configuring privilege level for BMC users using the Web UI</a> for further instructions on privilege level.</p>	 <p>The screenshot shows the "User Management Configuration" form. It includes fields for Username, Password Size (set to 16 bytes), Password, Confirm Password, and Enable User Access (checkboxes for Channel 1 and Channel 2, with Channel 1 checked).</p>
Step_5	Enable the user on the desired channel(s).	 <p>The screenshot shows the "Enable User Access" section of the configuration form. It has two checkboxes: "Channel 1" (checked) and "Channel 2".</p>
Step_6	Press <b>Save</b> to exit.	 <p>The screenshot shows the bottom right corner of the configuration form. It features a large red arrow pointing to the "Save" button, which is highlighted in blue.</p>

## Adding a BMC user using IPMI over LAN (IOL)

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

# PRELIMINARY

Step_1	<p>From a remote computer that has access to the management network subnet, print the list of users and select the ID of the user to add.</p> <pre>RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list</pre>	<pre># ipmitool -I lanplus -H 172.16.191.107 -U admin -P admin user list ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2  admin         false  false   true    ADMINISTRATOR 3              true   false  false    NO ACCESS 4              true   false  false    NO ACCESS 5              true   false  false    NO ACCESS 6              true   false  false    NO ACCESS 7              true   false  false    NO ACCESS 8              true   false  false    NO ACCESS 9              true   false  false    NO ACCESS 10             true  false  false    NO ACCESS</pre>
Step_2	<p>Create a user name.</p> <pre>RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user set name [IPMI user ID] [new IPMI user name]</pre> <p>NOTE: The first and second user names of the user list are reserved fields and therefore can't be modified.</p>	
Step_3	<p>Create the password.</p> <pre>RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user set password [IPMI user ID] [new IPMI password]</pre>	
Step_4	<p>Enable channel access and configure privilege level.</p> <pre>RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]</pre>	
Step_5	<p>Enable the user.</p> <pre>RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user enable [USER_ID]</pre>	

## Adding a BMC user using IPMI via KCS

Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

Step_1	<p>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.</p> <pre>LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]</pre>	<pre>[root@localhost ~]# ipmitool user list 1 ID Name          Callin Link Auth IPMI Msg Channel Priv Limit 1              false  false   true    ADMINISTRATOR 2  admin         false  false   true    ADMINISTRATOR 3              true   false  false    NO ACCESS 4              true   false  false    NO ACCESS 5              true   false  false    NO ACCESS 6              true   false  false    NO ACCESS 7              true   false  false    NO ACCESS 8              true   false  false    NO ACCESS 9              true   false  false    NO ACCESS 10             true  false  false    NO ACCESS</pre>
Step_2	<p>Create a user name.</p> <pre>LocalServer_OSPrompt:~# ipmitool user set name [IPMI user ID] [new IPMI user name]</pre> <p>NOTE: The first and second user names of the user list are reserved fields and therefore can't be modified.</p>	
Step_3	<p>Create the password.</p> <pre>LocalServer_OSPrompt:~# ipmitool user set password [IPMI user ID] [new IPMI password]</pre>	
Step_4	<p>Enable channel access and configure privilege level.</p> <pre>LocalServer_OSPrompt:~# ipmitool channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]</pre>	
Step_5	<p>Enable the user.</p> <pre>LocalServer_OSPrompt:~# ipmitool user enable [USER_ID]</pre>	

## Deleting or disabling a BMC user

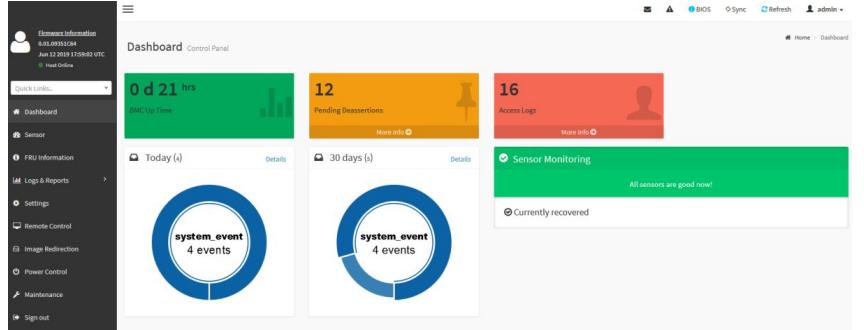
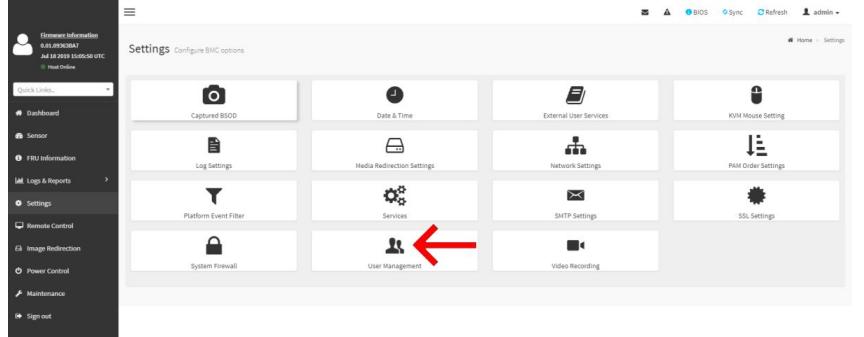
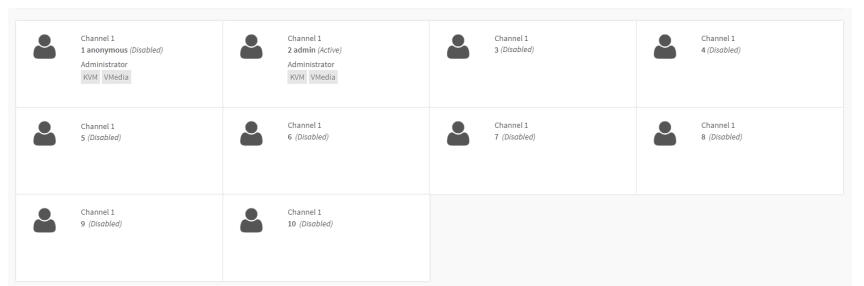
# PRELIMINARY

BMC users can be :

- Deleted using the [Web UI](#)
- Disabled using [IPMI over LAN \(IOL\)](#)
- Disabled using [IPMI via KCS](#)

## Deleting a BMC user using the Web UI

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

Step_1	<p>Access the BMC Web UI of the server.</p> 
Step_2	<p>Click on <b>Settings</b> in the left side menu and click on <b>User Management</b>.</p> 
Step_3	<p>Select the ID of the user to delete.</p> <p><b>NOTE:</b> The first and second users are reserved fields and therefore can't be deleted.</p> 
Step_4	<p>Press on <b>Delete</b> to delete the user.</p> 

## Disabling a BMC user using IPMI over LAN (IOL)

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

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

## PRELIMINARY

<p><b>Step_1</b></p> <p>From a remote computer that has access to the management network subnet, print the list of users and select the ID of the user to disable.</p> <pre>RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list</pre>	<pre>[root@localhost ~]# ipmitool user list 1 ID  Name          Callin  Link Auth  IPMI Msg  Channel Priv Limit 1   false         false    true      ADMINISTRATOR 2   admin         false    true      ADMINISTRATOR 3   true          false    false     NO ACCESS 4   true          false    false     NO ACCESS 5   true          false    false     NO ACCESS 6   true          false    false     NO ACCESS 7   true          false    false     NO ACCESS 8   true          false    false     NO ACCESS 9   true          false    false     NO ACCESS 10  true          false    false     NO ACCESS</pre>
<p><b>Step_2</b></p> <p>Disable the selected user.</p> <pre>RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user disable [USER_ID]</pre> <p>NOTE: The first and second user names of the user list are reserved fields and therefore can't be disabled.</p>	

### Disabling a BMC user using IPMI via KCS

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

Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

<p><b>Step_1</b></p> <p>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.</p> <pre>LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]</pre>	<pre>[root@localhost ~]# ipmitool user list 1 ID  Name          Callin  Link Auth  IPMI Msg  Channel Priv Limit 1   false         false    true      ADMINISTRATOR 2   admin         false    true      ADMINISTRATOR 3   true          false    false     NO ACCESS 4   true          false    false     NO ACCESS 5   true          false    false     NO ACCESS 6   true          false    false     NO ACCESS 7   true          false    false     NO ACCESS 8   true          false    false     NO ACCESS 9   true          false    false     NO ACCESS 10  true          false    false     NO ACCESS</pre>
<p><b>Step_2</b></p> <p>Disable the selected user.</p> <pre>LocalServer_OSPrompt:~# ipmitool user disable [USER_ID]</pre> <p>NOTE: The first and second user names of the user list are reserved fields and therefore can't be disabled.</p>	

### Configuring privilege level for BMC users

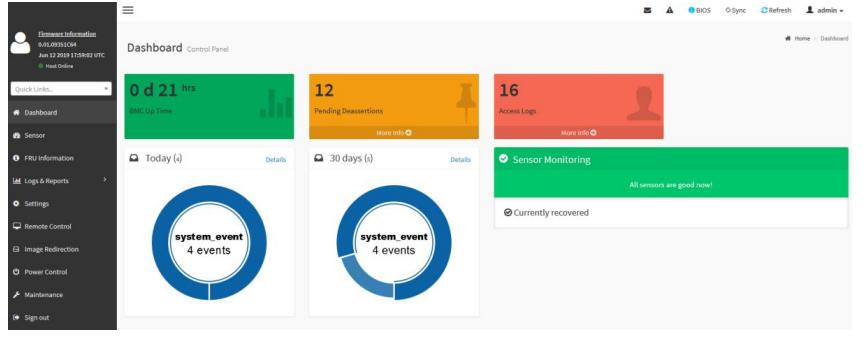
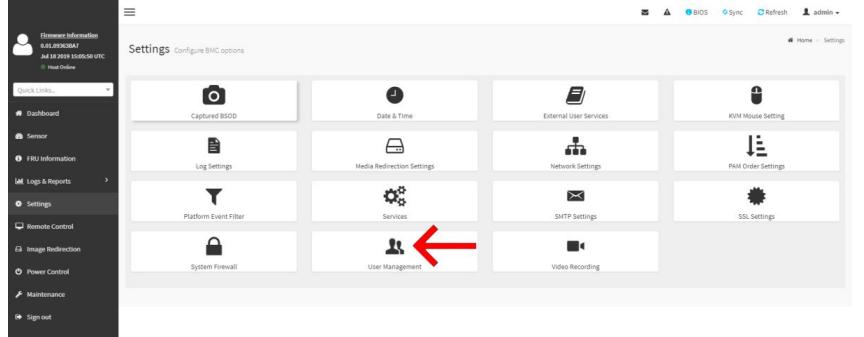
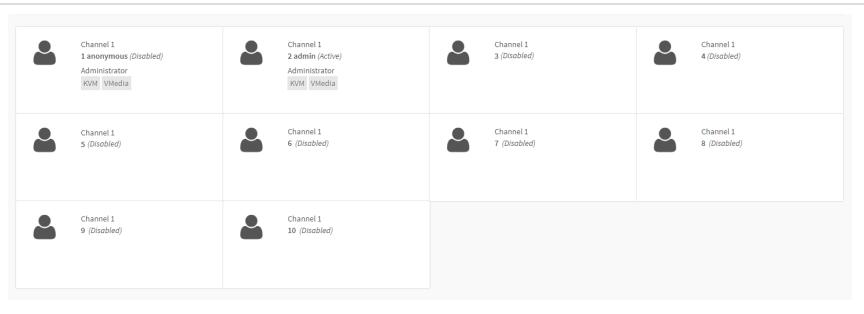
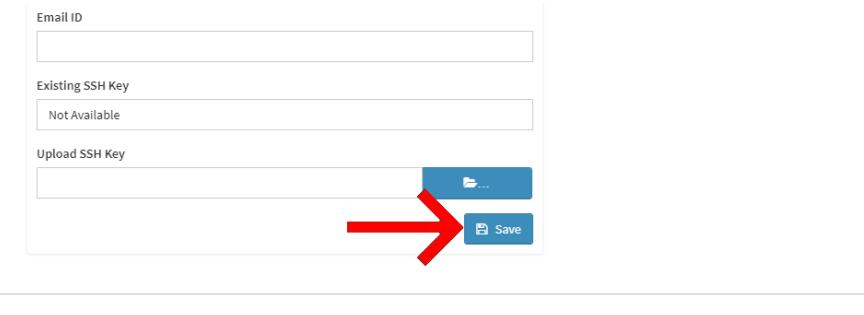
BMC user privilege level can be configured :

- Using the [Web UI](#)
- Using [IPMI over LAN \(IOL\)](#)
- Using [IPMI via KCS](#)

### Configuring privilege level for BMC users using the Web UI

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

# PRELIMINARY

Step_1	<p>Access the BMC Web UI of the server.</p> 
Step_2	<p>Click on <b>Settings</b> in the left side menu and click on <b>User Management</b>.</p> 
Step_3	<p>Select the ID of the user to manage.</p> <p><b>NOTE:</b> The first and second users are reserved fields and therefore can't be overwritten.</p> 
Step_4	<p>Configure the privilege level for each channel according to the application's requirements.</p> 
Step_5	<p>Press on <b>Save</b> to exit.</p> 

## Configuring privilege level for BMC users using IPMI over LAN (IOL)

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

# PRELIMINARY

<p><b>Step_1</b></p> <p>From a remote computer that has access to the management network subnet, print the list of users and select the ID of the user to manage.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list</pre>	<pre>[root@localhost ~]# ipmitool user list 1 ID  Name          Callin  Link Auth  IPMI Msg  Channel Priv Limit 1   false         false    true      ADMINISTRATOR 2   admin         false    true      ADMINISTRATOR 3   true          false    false     NO ACCESS 4   true          false    false     NO ACCESS 5   true          false    false     NO ACCESS 6   true          false    false     NO ACCESS 7   true          false    false     NO ACCESS 8   true          false    false     NO ACCESS 9   true          false    false     NO ACCESS 10  true          false    false     NO ACCESS</pre>
<p><b>Step_2</b></p> <p>List available privilege levels.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] channel help</pre>	<pre>Channel Commands: authcap &lt;channel number&gt; &lt;max privilege&gt; getaccess &lt;channel number&gt; [user id] setaccess &lt;channel number&gt; &lt;user id&gt; [callin=on off] [ipmi=on off] [link=on off] [privilege=level] info &lt;channel number&gt; getciphers &lt;ipmi   sol&gt; [channel] setkg hex/plain &lt;key&gt; [channel]  Possible privilege levels are: 1  Callback level 2  User level 3  Operator level 4  Administrator level 5  OEM Proprietary level 15 No access</pre>
<p><b>Step_3</b></p> <p>Set privilege level for each channel.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]</pre> <p>NOTE: The first and second user names of the user list are reserved fields and therefore can't be modified.</p>	

## Configuring privilege level for BMC users using IPMI via KCS

Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

<p><b>Step_1</b></p> <p>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.</p> <pre>LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]</pre>	<pre>[root@localhost ~]# ipmitool user list 1 ID  Name          Callin  Link Auth  IPMI Msg  Channel Priv Limit 1   false         false    true      ADMINISTRATOR 2   admin         false    true      ADMINISTRATOR 3   true          false    false     NO ACCESS 4   true          false    false     NO ACCESS 5   true          false    false     NO ACCESS 6   true          false    false     NO ACCESS 7   true          false    false     NO ACCESS 8   true          false    false     NO ACCESS 9   true          false    false     NO ACCESS 10  true          false    false     NO ACCESS</pre>
<p><b>Step_2</b></p> <p>List available privilege levels.</p> <pre>LocalServer_OSPrompt:~# ipmitool channel help</pre>	<pre>Channel Commands: authcap &lt;channel number&gt; &lt;max privilege&gt; getaccess &lt;channel number&gt; [user id] setaccess &lt;channel number&gt; &lt;user id&gt; [callin=on off] [ipmi=on off] [link=on off] [privilege=level] info &lt;channel number&gt; getciphers &lt;ipmi   sol&gt; [channel] setkg hex/plain &lt;key&gt; [channel]  Possible privilege levels are: 1  Callback level 2  User level 3  Operator level 4  Administrator level 5  OEM Proprietary level 15 No access</pre>
<p><b>Step_3</b></p> <p>Set privilege level for each channel.</p> <pre>LocalServer_OSPrompt:~# ipmitool channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]</pre> <p>NOTE: The first and second user names of the user list are reserved fields and therefore can't be modified.</p>	

## Managing Redfish users

### Configuring Redfish user names and passwords

Refer to [Accessing a BMC using Redfish](#) for access instructions.

## PRELIMINARY

Step_1	<p>Print the user list and select the ID of the user to modify.</p> <p>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]/AccountService/Accounts   jq</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts   jq {   "odata_context": "/redfish/v1/\$metadata#ManagerAccount_ManagerAccountCollection",   "odata_etag": "W/\"1563020241\"",   "odata_id": "/redfish/v1/AccountService/Accounts",   "odata_type": "#ManagerAccount.v1_1_0.ManagerAccount",   "Description": "Collection for Manager Accounts",   "Members": [     {       "odata_id": "/redfish/v1/AccountService/Accounts/1"     },     {       "odata_id": "/redfish/v1/AccountService/Accounts/4"     },     {       "odata_id": "/redfish/v1/AccountService/Accounts/2"     },     {       "odata_id": "/redfish/v1/AccountService/Accounts/5"     }   ],   "Members@odata.count": 4,   "Name": "Accounts Collection" }</pre>
Step_2	<p>Append the previous URL with the ID selected to display the user's information.</p> <p>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]/AccountService/Accounts/[USER_ID]   jq</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/1   jq {   "odata_context": "/redfish/v1/\$metadata#ManagerAccount_ManagerAccount",   "odata_etag": "W/\"1563020241\"",   "odata_id": "/redfish/v1/AccountService/Accounts/1",   "odata_type": "#ManagerAccount.v1_1_0.ManagerAccount",   "Description": "Default Account",   "Enabled": true,   "Id": "1",   "Links": [     {       "odata_id": "/redfish/v1/AccountService/Roles/Administrator"     }   ],   "Locked": false,   "Name": "Default Account",   "Notes": "Administrator",   "UserName": "Administrator" }</pre>
Step_3	<p>Print the ETag of the URL of the desired account.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] -X HEAD -i   grep ETag</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/1 -X HEAD -i   grep ETag</pre>
Step_4	<p>Change the user name if necessary.</p> <p>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]/AccountService/Accounts/[USER_ID] -X PATCH -d '{"UserName":"[NEW_USERNAME]"}' -H 'If-Match: [ETAG_VALUE]' -H 'Content-type: application/json'   jq</p> <p>NOTE: Once the user name is modified, it needs to be updated in the ROOT_URL.</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/1 -X PATCH -d '{"UserName":"[NEW_USERNAME]"}' -H 'If-Match: W/\"1563809678\" -H 'Content-type: application/json'   jq</pre>
Step_5	<p>Print the ETag of the URL of the desired account.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] -X HEAD -i   grep ETag</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/1 -X HEAD -i   grep ETag ETag: W/\"1564494159"</pre>
Step_6	<p>Change the password if necessary.</p> <p>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]/AccountService/Accounts/[USER_ID] -X PATCH -d '{"Password":"[NEW_PASSWORD]"}' -H 'If-Match: [ETAG_VALUE]' -H 'Content-type: application/json'   jq</p> <p>NOTE: Once the password is modified, it needs to be updated in the ROOT_URL.</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/1 -X PATCH -d '{"Password":"[NewPassword]"}' -H 'If-Match: W/\"1564494159\" -H 'Content-type: application/json'   jq</pre>
Step_7	<p>Verify that the credentials updated correctly by opening a new session in the Redfish API.</p>	

### Adding a Redfish user

Refer to [Accessing a BMC using Redfish](#) for access instructions.

## PRELIMINARY

Step_1	<p>Append the Root URL with the AccountService/Accounts suffix.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts   jq</p>	<pre>\$ curl -k -s -g https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts   jq {   "odata.context": "/redfish/v1/odata/ManagerAccountCollection.ManagerAccountCollection",   "odata.etag": "W/\"1564427308\"",   "odata.id": "/redfish/v1/AccountService/Accounts",   "odata.type": "#ManagerAccountCollection.ManagerAccountCollection",   "Description": "Collection For Manager Accounts",   "Members": [     {       "odata.id": "/redfish/v1/AccountService/Accounts/1"     },     {       "odata.id": "/redfish/v1/AccountService/Accounts/3"     }   ],   "Members@odata.count": 2,   "Name": "Accounts Collection" }</pre>
Step_2	<p>Create the user and get its ID in the response message.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts -X POST -d '{"Password":" [PASSWORD] ","RoleId":" [ROLE_ID] ","UserName":" [USER_NAME] "}' -H "Content-Type: application/json"   jq</p> <p>NOTE: The ID of the user will be automatically created.</p>	<pre>\$ curl -k -s -g https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts -X POST -d '{"Password":"operator","RoleId":"Operator","UserName":"operator"}' -H "Content-Type: application/json"   jq {   "odata.context": "/redfish/v1/odata/ManagerAccountCollection",   "odata.etag": "W/\"1564427308\"",   "odata.id": "/redfish/v1/AccountService/Accounts",   "odata.type": "#ManagerAccountCollection.v1_1_2.ManagerAccountCollection",   "Description": "Collection of Account Details",   "Members": [     {       "odata.id": "/redfish/v1/AccountService/Accounts/6"     }   ],   "Members@odata.count": 1,   "Name": "Accounts Collection" }</pre>
Step_3	<p>Print the ETag of the URL of the account created.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] -X HEAD -i   grep ETag</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/6 -X HEAD -i   grep ETag ETag: W/"1564427308"</pre>
Step_4	<p>Enable the user.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] -X PATCH -d '{"Enabled":true}' -H 'If-Match: [ETAG_VALUE]' -H 'Content-type: application/json'   jq</p>	<pre>\$ curl -s -k https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/6 -X PATCH -d '{"Enabled":true}' -H 'If-Match: W/"1564427308"' -H 'Content-type: application/json'   jq {   "odata.context": "/redfish/v1/odata/ManagerAccountCollection",   "odata.etag": "W/\"1564427308\"",   "odata.id": "/redfish/v1/AccountService/Accounts/6",   "odata.type": "#ManagerAccountCollection.v1_1_2.ManagerAccountCollection",   "Description": "Collection For Manager Accounts",   "Members": [     {       "odata.id": "/redfish/v1/AccountService/Accounts/1"     },     {       "odata.id": "/redfish/v1/AccountService/Accounts/3"     }   ],   "Members@odata.count": 2,   "Name": "Accounts Collection" }</pre>
Step_5	<p>Verify that the user was created correctly by connecting to Redfish using its credentials.</p>	

## Deleting a Redfish user

Refer to [Accessing a BMC using Redfish](#) for access instructions.

Step_1	<p>Append the Root URL with the AccountService/Accounts suffix and select the user to delete.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts   jq</p>	<pre>\$ curl -s -k https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts   jq {   "odata.context": "/redfish/v1/odata/ManagerAccountCollection.ManagerAccountCollection",   "odata.etag": "W/\"1564427308\"",   "odata.id": "/redfish/v1/AccountService/Accounts",   "odata.type": "#ManagerAccountCollection.ManagerAccountCollection",   "Description": "Collection For Manager Accounts",   "Members": [     {       "odata.id": "/redfish/v1/AccountService/Accounts/1"     },     {       "odata.id": "/redfish/v1/AccountService/Accounts/3"     }   ],   "Members@odata.count": 2,   "Name": "Accounts Collection" }</pre>
Step_2	<p>Delete the user.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] -X DELETE   jq</p>	<pre>\$ curl -s -k https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/7 -X DELETE   jq {   "odata.context": "/redfish/v1/odata/ManagerAccountCollection",   "odata.etag": "W/\"1564427308\"",   "odata.id": "/redfish/v1/AccountService/Accounts",   "odata.type": "#ManagerAccountCollection.ManagerAccountCollection",   "Description": "Collection For Manager Accounts",   "Members": [     {       "odata.id": "/redfish/v1/AccountService/Accounts/1"     },     {       "odata.id": "/redfish/v1/AccountService/Accounts/3"     }   ],   "Members@odata.count": 2,   "Name": "Accounts Collection" }</pre>
Step_3	<p>Verify that the user has been deleted properly.</p> <p>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts   jq</p>	<pre>\$ curl -s -k https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts   jq {   "odata.context": "/redfish/v1/odata/ManagerAccountCollection",   "odata.etag": "W/\"1564427308\"",   "odata.id": "/redfish/v1/AccountService/Accounts",   "odata.type": "#ManagerAccountCollection.ManagerAccountCollection",   "Description": "Collection For Manager Accounts",   "Members": [     {       "odata.id": "/redfish/v1/AccountService/Accounts/1"     },     {       "odata.id": "/redfish/v1/AccountService/Accounts/3"     }   ],   "Members@odata.count": 2,   "Name": "Accounts Collection" }</pre>

## Configuring Redfish privilege level

Refer to [Accessing a BMC using Redfish](#) for access instructions.

## PRELIMINARY

<p><b>Step_1</b></p> <p>Append the Root URL with the AccountService/Accounts suffix and select the desired user.</p> <pre>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts   jq</pre>	<pre>\$ curl -s -k https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts   jq {   "odata.context": "/redfish/v1/AccountService/ManagerAccountCollection",   "odata.type": "#ManagerAccountCollection.ManagerAccountCollection",   "odata.id": "/redfish/v1/AccountService/Accounts",   "Members": [     {       "odata.id": "/redfish/v1/AccountService/Accounts/1"     },     {       "odata.id": "/redfish/v1/AccountService/Accounts/3"     },     {       "odata.id": "/redfish/v1/AccountService/Accounts/8"     }   ],   "Members@odata.count": 3,   "Name": "Accounts Collection" }</pre>
<p><b>Step_2</b></p> <p>Print the ETag of the URL of the desired account.</p> <pre>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] -X HEAD -i   grep ETag</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/8 -X HEAD -i   grep ETag ETag: W/"1564431523"</pre>
<p><b>Step_3</b></p> <p>Set the privilege level.</p> <pre>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] -X PATCH -d '{"RoleId": " [ROLE_ID ]"}' -H 'If- Match: [ETAG_VALUE]' -H 'Content-type: application/json'   jq</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/8 -X PATCH -d '{"RoleId": "Administrator"}' -H 'If-Match: W/"1564431523"' -H 'Content-type: application/json'   jq</pre>
<p><b>Step_4</b></p> <p>Verify that the RoleID has updated properly.</p> <pre>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID]   jq</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/AccountService/Accounts/8   jq {   "odata.context": "/redfish/v1/AccountService/ManagerAccount",   "odata.etag": "W/\"1564431523\"",   "odata.id": "/redfish/v1/AccountService/Accounts/8",   "odata.type": "#ManagerAccount.v1_1_2.ManagerAccount",   "Description": "A collection of Account details",   "Enabled": false,   "Id": "8",   "Links": {     "Role": {       "odata.id": "/redfish/v1/AccountService/Roles/Administrator"     }   },   "Locked": false,   "Name": "Operator",   "RoleId": "Administrator",   "UserName": "Operator" }</pre>

## Configuring SNMP users using BMC SNMP

BMC SNMP users are shared with BMC users.

- To configure a user, refer to [Configuring BMC users](#).
- To enable or disable SNMP access, refer to [Configuring BMC SNMP](#).

## Configuring OS users

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

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

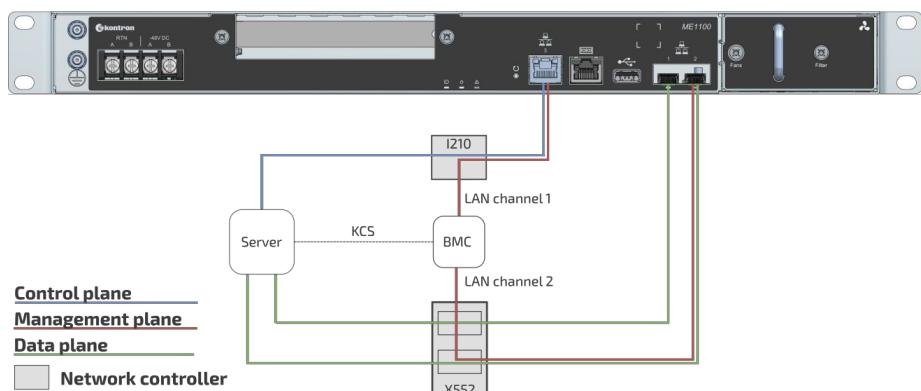
# Baseboard management controller – BMC

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

## Table of contents

- [BMC architecture](#)
- [Selecting an access method](#)
- [Discovering the platform management IP address](#)
  - [Discovering the platform management IP address with DHCP Dynamic DNS update](#)
    - [Prerequisites](#)
    - [Procedure](#)
  - [Discovering the platform management IP address using the BIOS](#)
    - [Accessing the BIOS using a serial console \(physical connection\)](#)
    - [Accessing the BMC network configuration menu](#)
  - [Discovering the platform management IP address using DHCP server logs](#)
    - [Prerequisites](#)
- [Configuring a static IP address](#)
  - [Configuring a static IP address using the BIOS setup menu](#)
    - [Accessing the BIOS setup menu](#)
    - [Accessing the BMC network configuration menu](#)
    - [Configuring a static IP address](#)
  - [Configuring a static IP address using IPMI](#)
    - [Accessing the BMC](#)
    - [Configuring a static IP address](#)
- [Configuring a dynamic IP address using DHCP](#)
  - [Configuring a dynamic IP address using the BIOS setup menu](#)
    - [Accessing the BIOS setup menu](#)
    - [Accessing the BMC network configuration menu](#)
    - [Configuring a dynamic IP address using DHCP](#)
  - [Configuring a dynamic IP address using IPMI](#)
    - [Accessing the BMC](#)
    - [Configuring a dynamic IP address](#)

## BMC architecture



- The network configuration allows for setting the two BMC LAN ports (channel 1 and channel 2) either on different networks or on the same network.
  - Two management IP addresses can be configured for the ME1100 platform: one for LAN channel 1 (RJ45 connector – port 3); and one for LAN channel 2 (SFP connector – port 2).
  - By default, the IP addresses of the network interfaces of the BMC are obtained through the DHCP protocol.
- Refer to [Product architecture](#) for more information on network connectivity.

## Selecting an access method

The BMC can be configured using various access methods depending on specific parameters.

- If the **BMC IP address** is **unknown** and there is **no OS installed** :
  - Use the BIOS setup menu
- If the **BMC IP address** is **unknown** and an **OS is installed** :
  - Use IPMI via KCS
  - Use the BIOS setup menu
- If the **BMC IP address** is **known** and an **OS is installed** :
  - Use IPMI (KCS or IOL)
  - Use the BIOS setup menu

## Discovering the platform management IP address

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

The management IP address can be discovered:

- Using [DHCP Dynamic DNS update](#)
- Using the [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 management IP address with DHCP Dynamic DNS update

#### Prerequisites

1	A DHCP server with active Dynamic DNS update feature is available.
2	A remote computer configured with the same DNS server is available.
3	The MAC address of the BMC (BMC RJ45 port 3; or BMC SFP port 2) is known.

Relevant section:

[MAC addresses](#)

#### Procedure

When requesting a DHCP lease, the platform BMC supplies the DHCP server with information to update the DNS system. If the DHCP server is configured for Dynamic DNS update, an entry will be added for a host name that is made up of the "ME1100" prefix and the BMC MAC address.

For example, if we use the MAC address discovered for BMC RJ45 port 3 of the ME1100 (i.e. 00:a0:a5:d2:e9:0a , refer to section [MAC addresses](#) ), the host name would be: ME1100\_00A0A5D2E90A .

The following example illustrates the method using DNS auto-registration with a remote computer that has access to the DHCP server network.

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

### Discovering the platform management IP address using the BIOS

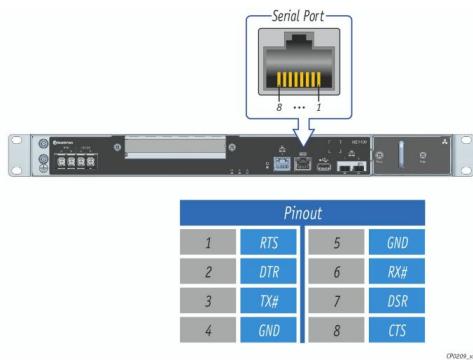
# PRELIMINARY

## Accessing the BIOS using a serial console (physical connection)

### Prerequisites

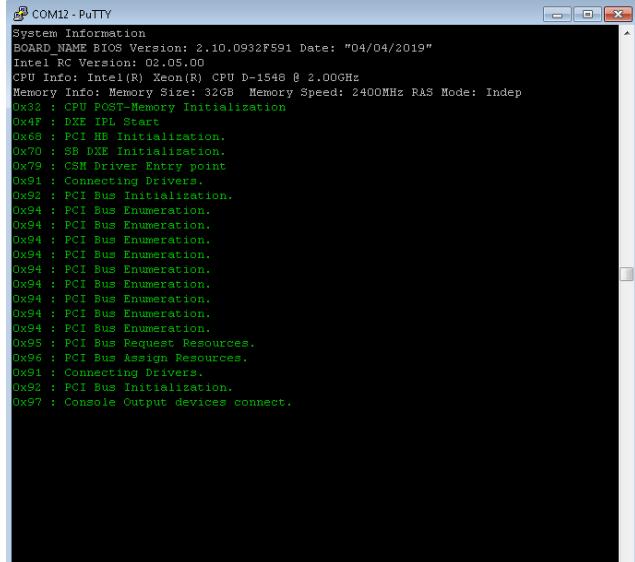
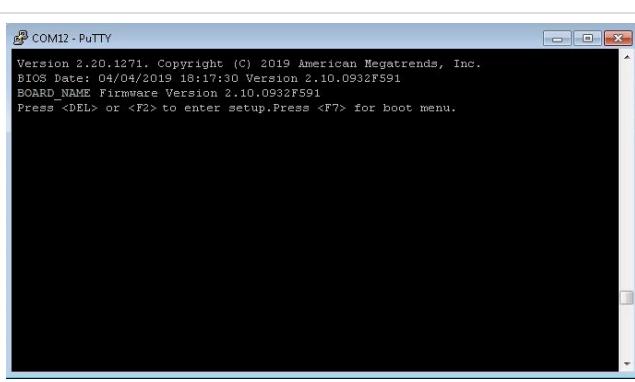
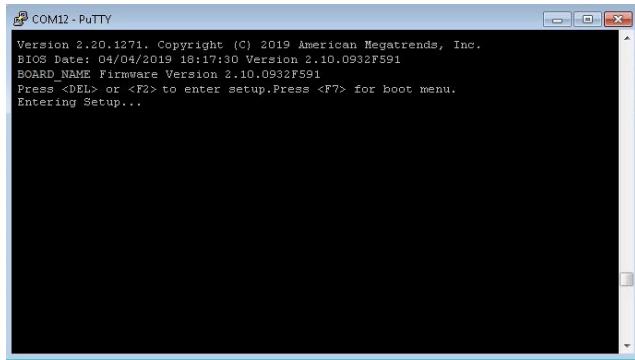
1	A physical connection to the device is required. <b>NOTE:</b> The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the external computer. <ul style="list-style-type: none"><li>• Speed (Baud): 115200</li><li>• Data bits: 8</li><li>• Stop bits: 1</li><li>• Parity: None</li><li>• Flow Control: None</li><li>• Recommended emulation mode: VT100+</li></ul> <b>NOTE:</b> PuTTY is recommended.

### Port location



### Access procedure

## PRELIMINARY

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.	 <pre>COM12 - PuTTY System Information BOARD_NAME BIOS Version: 2.10.0932F591 Date: "04/04/2019" Intel RC Version: 02.05.00 CPU Info: Intel(R) Xeon(R) CPU D-1548 @ 2.00GHz Memory Info: Memory Size: 32GB Memory Speed: 2400MHz RAS Mode: Indep 0x32 : CPU POST-Memory Initialization 0x4F : DXE IPL Start 0x68 : PCI HB Initialization. 0x70 : SB DXE Initialization. 0x79 : CSM Driver Entry point 0x91 : Connecting Drivers. 0x92 : PCI Bus Initialization. 0x94 : PCI Bus Enumeration. 0x95 : PCI Bus Request Resources. 0x96 : PCI Bus Assign Resources. 0x91 : Connecting Drivers. 0x92 : PCI Bus Initialization. 0x97 : Console Output devices connect.</pre>
Step_2	<p>Perform a server reset (<b>Ctrl-break</b> hot key).</p> <p><b>NOTE:</b> If an operating system is installed on the device, the hot key might not work properly. If this is the case, reset the server as recommended for the operating system.</p> <p><b>NOTE:</b> When a server reset command is sent, it may take a few seconds for the BIOS sign on screen to display.</p>	 <pre>COM12 - PuTTY Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. BIOS Date: 04/04/2019 18:17:30 Version 2.10.0932F591 BOARD_NAME Firmware Version 2.10.0932F591 Press &lt;DEL&gt; or &lt;F2&gt; to enter setup.Press &lt;F7&gt; for boot menu.</pre>
Step_3	<p>When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.</p> <p><b>NOTE:</b> It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup...".</p>	 <pre>COM12 - PuTTY Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. BIOS Date: 04/04/2019 18:17:30 Version 2.10.0932F591 BOARD_NAME Firmware Version 2.10.0932F591 Press &lt;DEL&gt; or &lt;F2&gt; to enter setup.Press &lt;F7&gt; for boot menu. Entering Setup...</pre>
Step_4	<p>The BIOS sign on screen displays "Entering Setup...".</p> <p><b>NOTE:</b> It will take several seconds to display and enter the BIOS setup menu.</p>	<pre>COM12 - PuTTY Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. BIOS Date: 04/04/2019 18:17:30 Version 2.10.0932F591 BOARD_NAME Firmware Version 2.10.0932F591 Press &lt;DEL&gt; or &lt;F2&gt; to enter setup.Press &lt;F7&gt; for boot menu. Entering Setup...</pre>
Step_5	The BIOS setup menu is displayed.	 <pre>APTIO Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IntelRCSetup Server Mgmt Security Boot Event Logs &gt; BIOS Information BIOS Vendor American Megatrends  Choose the system Core Version 5.14  default language Compliance UEFI 2.6: PI 1.4   Project Version x64   Build Date and Time 04/04/2019 18:17:30   Access Level Administrator   FPGA Version 2.02.0800AD12  --&gt; Select Screen Memory Information Total Memory 32768 MB  ^v: Select Item System Language [English]  Enter: Select System Date [Wed 06/26/2019]  +/-.: Change Opt. System Time [20:13:00]  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save &amp; Exit  ESC: Exit Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</pre>

### Accessing the BMC network configuration menu

**NOTE:** LAN channel 1 corresponds to the RJ45 connector (port 3) and LAN channel 2 corresponds to the SFP connector

# PRELIMINARY

(port 2).

Step_1	<p>From the BIOS menu, use the arrow keys to select <b>Server Mgmt</b>.</p>
Step_2	<p>Use the arrow keys to select <b>BMC network configuration</b>.</p>
Step_3	<p>The <b>BMC network configuration</b> menu is displayed.</p> <p><b>NOTE:</b> When the platform is powered up after being shut off, the BIOS may load before the BMC has received its IP address. In this case, the BIOS menu information will need to be refreshed by restarting the server and re-entering the BIOS.</p>

## Discovering the platform management IP address using DHCP server logs

### Prerequisites

1	Access to the DHCP server logs.
2	The MAC address of the BMC (BMC RJ45 port 3; or BMC SFP port 2) is known.

### Procedure

#### Relevant section:

[MAC addresses](#)

## PRELIMINARY

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

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

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

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

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

## Configuring a static IP address



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

A static IP address can be configured:

- Using the [BIOS setup menu](#)
- Using [IPMI](#)

### Configuring a static IP address using the BIOS setup menu

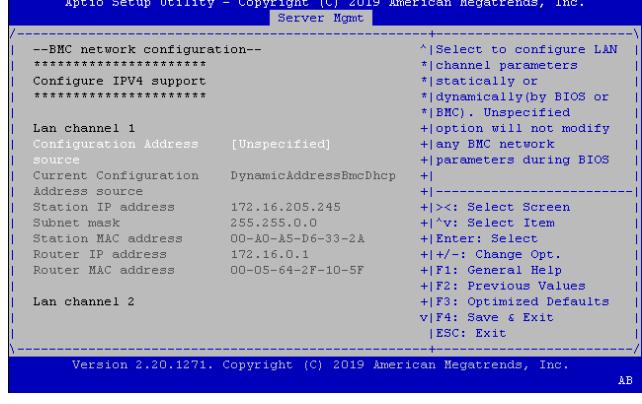
#### Accessing the BIOS setup menu

The BIOS setup menu can be accessed using various methods:

- If there is no OS installed and no known IP address, it is mandatory to use a serial console. Refer to [Accessing the BIOS using a serial console \(physical connection\)](#).
- If the IP address of the BMC is known, any BIOS access methods will work. Refer to [Accessing the BIOS](#) to choose an access method.

#### Accessing the BMC network configuration menu

# PRELIMINARY

Step_1	<p>From the BIOS menu, use the arrow keys to select <b>Server Mgmt</b>.</p>	 <p>The screenshot shows the Aptio Setup Utility main menu. The 'Server Mgmt' tab is highlighted in yellow. Other tabs include Main, Advanced, IntelRCSsetup, Security, Boot, and Event Logs. The BIOS information section displays details like BIOS Vendor (American Megatrends), Core Version (5.14), and System Date (Wed 07/10/2019). A legend on the right explains key functions: F1 for General Help, F2 for Previous Values, F3 for Optimized Defaults, F4 for Save &amp; Exit, and ESC for Exit.</p>
Step_2	<p>Use the arrow keys to select <b>BMC network configuration</b>.</p>	 <p>The screenshot shows the BMC network configuration menu. The 'BMC network configuration' option is highlighted in yellow. Other options include System Event Log, View FRU information, and BMC User Settings. A legend on the right explains key functions: F1 for General Help, F2 for Previous Values, F3 for Optimized Defaults, F4 for Save &amp; Exit, and ESC for Exit.</p>
Step_3	<p>The BMC network configuration menu is displayed.</p> <p><b>NOTE:</b> When the platform is powered up after being shut off, the BIOS may load before the BMC has received its IP address. In this case, the BIOS menu information will need to be refreshed by restarting the server and re-entering the BIOS.</p>	 <p>The screenshot shows the BMC network configuration menu. The 'BMC network configuration' option is highlighted in yellow. Other options include LAN channel 1 and LAN channel 2. A legend on the right explains key functions: F1 for General Help, F2 for Previous Values, F3 for Optimized Defaults, F4 for Save &amp; Exit, and ESC for Exit.</p>

## Configuring a static IP address

**NOTE:** LAN channel 1 corresponds to the RJ45 connector (port 3) and LAN channel 2 corresponds to the SFP connector (port 2).

# PRELIMINARY

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).	<pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Server Ngmt  /-----BMC network configuration----- *****Configure IPv4 support***** *****Lan channel 1***** Configuration Address source [Unspecified] Current Configuration DynamicAddressBmcDhcp Address source Station IP address 172.16.205.245 Subnet mask 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 172.16.0.1 Router MAC address 00-05-64-2F-10-5F  *****Lan channel 2***** Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. </pre>
Step_2	Select Static.	<pre> /---- Configuration Address source ---\   Unspecified   <b>Static</b>   DynamicBmcDhcp   DynamicBmcNonDhcp \-----/ </pre>
Step_3	Change the Station IP address . NOTE: This is the management IP address ( BMC MNGMT_IP ).	<pre> Lan channel 1 Configuration Address source [Static] Station IP address /--Station IP address--\ 172.16.205.245 Subnet mask \-----\ 00 Station MAC address Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00-00 </pre>
Step_4	Change the Subnet mask .	<pre> Lan channel 1 Configuration Address source [Static] Station IP address /---Subnet mask---\ 1255.255.0.0 Subnet mask \-----\ 00 Station MAC address Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00-00 </pre>
Step_5	(Optional) Change the Router IP address .	<pre> Lan channel 1 Configuration Address source [Static] Station IP address /--Router IP address--\ 172.16.0.1 Subnet mask \-----\ 00 Station MAC address Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00-00 </pre>
Step_6	Confirm the configuration has changed and exit BMC network configuration using the ESC key.	<pre> Lan channel 1 Configuration Address source [Static] Station IP address 172.16.205.245 Subnet mask 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 172.16.0.1 Router MAC address 00-05-64-2F-10-5F </pre>

## Configuring a static IP address using IPMI

### Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to [Accessing a BMC on an ME module using IPMI \(KCS\)](#).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#).

The following procedures will be executed using the [Accessing a BMC on an ME module using IPMI \(KCS\)](#) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: **-l lanplus -H [BMC MNGMT\_IP] -U [IPMI user name] -P [IPMI password]** .

### Configuring a static IP address

## PRELIMINARY

**NOTE:** LAN channel 1 corresponds to the RJ45 connector (port 3) and LAN channel 2 corresponds to the SFP connector (port 2).

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] <b>NOTE:</b> This is the management IP address ( BMC MNGMT_IP ). <b>NOTE:</b> It can take several seconds for an IP address to be set.	[root@localhost ~]# ipmitool lan set 1 ipaddr 172.16.205.245 Setting LAN IP Address to 172.16.205.245
Step_3	Set the subnet mask. LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] netmask [NEW_MASK] <b>NOTE:</b> It can take several seconds for a subnet mask to be set.	[root@localhost ~]# ipmitool lan set 1 netmask 255.255.0.0 Setting LAN Subnet Mask to 255.255.0.0
Step_4	Set the default gateway IP address. LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] defgw ipaddr [ROUTER_IP] <b>NOTE:</b> It can take several seconds for a default gateway IP address to be set.	[root@localhost ~]# ipmitool lan set 1 defgw ipaddr 172.16.0.1 Setting LAN Default Gateway IP to 172.16.0.1
Step_5	Set the default gateway MAC address. LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] defgw macaddress [ROUTER_MAC]	[root@localhost ~]# ipmitool lan set 1 defgw macaddress 00:05:64:2f:10:5f Setting LAN Default Gateway MAC to 00:05:64:2f:10:5f
Step_6	Verify that the configuration has changed. LocalServer_OSPrompt:~# ipmitool lan print [LAN_CHANNEL]	[root@localhost ~]# ipmitool lan print 1 Set in Progress : Set Complete Auth Type Support : NONE PASSWORD Auth Type Enable : Callback : : User : NONE PASSWORD : Operator : PASSWORD : Admin : PASSWORD : OEM : IP Address Source : Static Address IP Address : 172.16.205.245 Subnet Mask : 255.255.0.0 MAC Address : 00:a5:d6:33:2a SNMP Community String : AMI IP Header : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10 BMC ARP Control : ARP Responses Enabled, Gratuitous ARP Disabled Gratuitous ARP Intrvl : 0.0 seconds Default Gateway IP : 172.16.0.1 Default Gateway MAC : 00:05:64:2f:10:5f Backup Gateway IP : 0.0.0.0 Backup Gateway MAC : 00:00:00:00:00:00 802.1q VLAN ID : Disabled 802.1q VLAN Priority : 0 RMCPlus Cipher Suites : 0,1,2,3,6,7,8,11,12,15,16,17 Cipher Suite Priv Max : caaaaaaaaaaaaXXX : X=Cipher Suite Unused : c=CALLBACK : u=USER : o=OPERATOR : a=ADMIN : O=OEM Bad Password Threshold : 0 Invalid password disable: no Attempt Count Reset Int.: 0 User Lockout Interval : 0

## Configuring a dynamic IP address using DHCP



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

A dynamic IP address can be configured:

# PRELIMINARY

- Using the [BIOS setup menu](#)
- Using [IPMI](#)

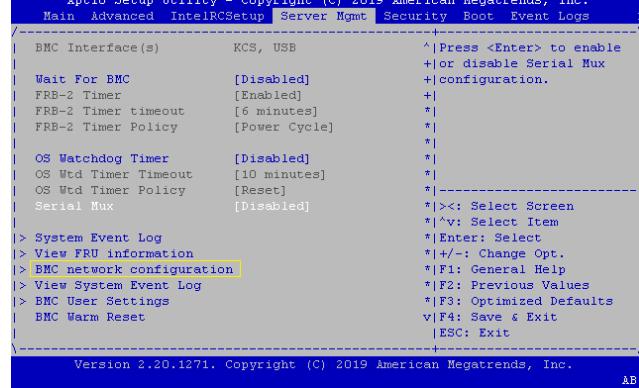
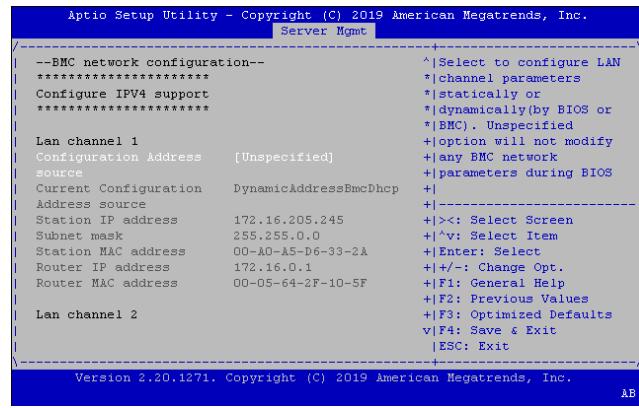
## Configuring a dynamic IP address using the BIOS setup menu

### Accessing the BIOS setup menu

The BIOS setup menu can be accessed using various methods:

- If there is no OS installed and no known IP address, it is mandatory to use a serial console. Refer to [Accessing the BIOS using a serial console \(physical connection\)](#).
- If the IP address of the BMC is known, any BIOS access methods will work. Refer to [Accessing the BIOS](#) to choose an access method.

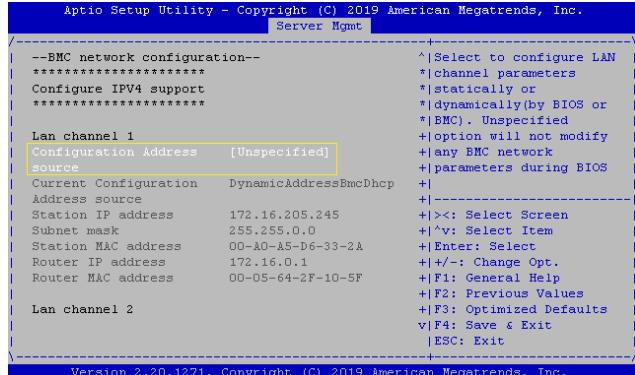
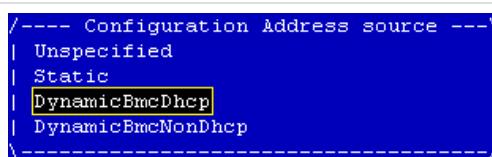
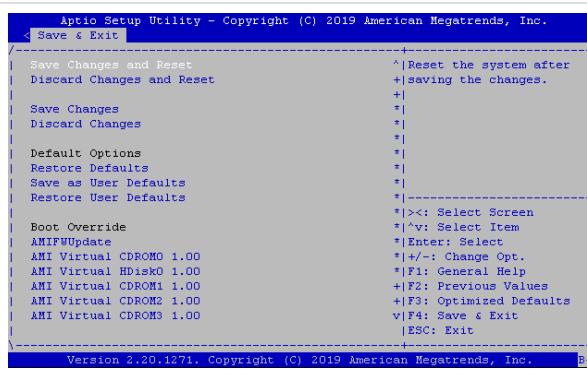
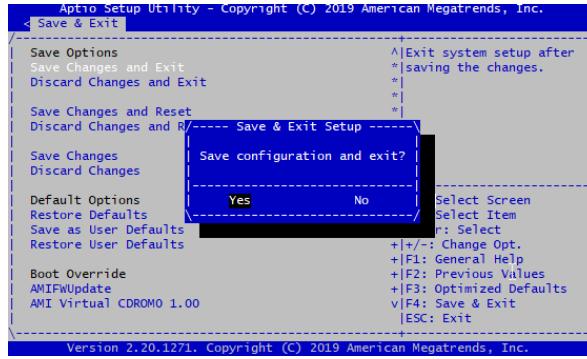
### Accessing the BMC network configuration menu

Step_1	From the BIOS menu, use the arrow keys to select Server Mgmt .	 <p>The screenshot shows the Aptio Setup Utility main menu with the "Server Mgmt" tab highlighted. The menu includes tabs for Main, Advanced, IntelRCSetup, Server Mgmt (highlighted), Security, Boot, and Event Logs. Below the tabs, there are sections for BIOS Information, Memory Information, and System Language, each with various configuration options and status information. A legend on the right provides keyboard shortcuts for navigation.</p>
Step_2	Use the arrow keys to select BMC network configuration .	 <p>The screenshot shows the Aptio Setup Utility main menu with the "Server Mgmt" tab highlighted. The menu includes tabs for Main, Advanced, IntelRCSetup, Server Mgmt (highlighted), Security, Boot, and Event Logs. Below the tabs, there are sections for BMC Interface(s), Wait For BMC, OS Watchdog Timer, and Serial Mux, each with various configuration options and status information. A legend on the right provides keyboard shortcuts for navigation.</p>
Step_3	The BMC network configuration menu is displayed. <b>NOTE:</b> When the platform is powered up after being shut off, the BIOS may load before the BMC has received its IP address. In this case, the BIOS menu information will need to be refreshed by restarting the server and re-entering the BIOS.	 <p>The screenshot shows the BMC network configuration menu. It starts with a section titled "--BMC network configuration--". Below this, there are sections for Configure IPv4 support, Lan channel 1, and Lan channel 2. Each section contains configuration parameters like Address source, Station IP address, Subnet mask, Station MAC address, Router IP address, and Router MAC address. A legend on the right provides keyboard shortcuts for navigation.</p>

## Configuring a dynamic IP address using DHCP

# PRELIMINARY

**NOTE:** LAN channel 1 corresponds to the RJ45 connector (port 3) and LAN channel 2 corresponds to the SFP connector (port 2).

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

## Configuring a dynamic IP address using IPMI

### Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to [Accessing a BMC on an ME module using IPMI \(KCS\)](#).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#).

The following procedures will be executed using the [Accessing a BMC on an ME module using IPMI \(KCS\)](#) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H

# PRELIMINARY

[BMC MNGMT\_IP] -U [IPMI user name] -P [IPMI password] .

## Configuring a dynamic IP address

NOTE: LAN channel 1 corresponds to the RJ45 connector (port 3) and LAN channel 2 corresponds to the SFP connector (port 2).

Step_1	<p>Set the IP source to DHCP.</p> <pre>LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] ipsrc dhcp</pre> <p><b>NOTE:</b> Depending on the existing infrastructure, it may take several seconds to gather an IP from the DHCP server.</p>	
Step_2	<p>Verify that the configuration has changed.</p> <pre>LocalServer_OSPrompt:~# ipmitool lan print [LAN_CHANNEL]</pre> <p><b>NOTE:</b> This is the management IP address ( BMC MNGMT_IP ).</p>	<pre>[root@localhost ~]# ipmitool lan print 1 Set in Progress      : Set Complete Auth Type Support   : NONE PASSWORD Auth Type Enable     : Callback            : User                : NONE PASSWORD Operator             : PASSWORD Admin               : PASSWORD OEM                 : IP Address Source   : DHCP Address IP Address          : 172.16.205.245 Subnet Mask         : 255.255.0.0 MAC Address          : 00:a0:a5:d6:33:2a SNMP Community String  : AMI IP Header           : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10 BMC ARP Control    : ARP Responses Enabled, Gratuitous ARP Disabled Gratuitous ARP Intrvl  : 0.0 seconds Default Gateway IP  : 172.16.0.1 Default Gateway MAC : 00:0c:29:95:98:42 Backup Gateway IP   : 0.0.0.0 Backup Gateway MAC  : 00:00:00:00:00:00 S02.1q VLAN ID     : Disabled S02.1q VLAN Priority : 0 RMCP+ Cipher Suites: 0,1,2,3,6,7,8,11,12,15,16,17 Cipher Suite Priv Max: caaaaaaaaaaaXXX                         : X=Cipher Suite Unused                         : c=CALLBACK                         : u=USER                         : o=OPERATOR                         : a=ADMIN                         : O=OEM Bad Password Threshold : 0 Invalid password disable: no Attempt Count Reset Int.: 0 User Lockout Interval  : 0</pre>

# Configuring the network time protocol - NTP

{This article describes how to configure NTP using different methods.}

Table of contents

- [Configuring the NTP using the Web UI](#)
  - [Prerequisites](#)
  - [Procedure](#)
- [Configuring the NTP using IPMI \(IOL or KCS\)](#)
  - [Prerequisites \(IOL\)](#)
  - [Prerequisites \(KCS\)](#)
  - [Getting the BMC time and date](#)
  - [Setting the BMC time and date](#)
  - [Confirming configuration](#)
  - [Step\\_1 Get the BMC time and date. LocalServer\\_OSPrompt:~# ipmitool sel time get Step\\_2 Verify that the BMC time and date match with the local time and date. NOTE: It may take several seconds or minutes before the BMC synchronizes time with the NTP server.](#)
  - [Decoding NTP raw configuration data](#)

The network time protocol (NTP) can be configured:

- Using the [Web UI](#)
- Using [IPMI \(IOL or KCS\)](#)



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

## Configuring the NTP using the Web UI

### Prerequisites

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

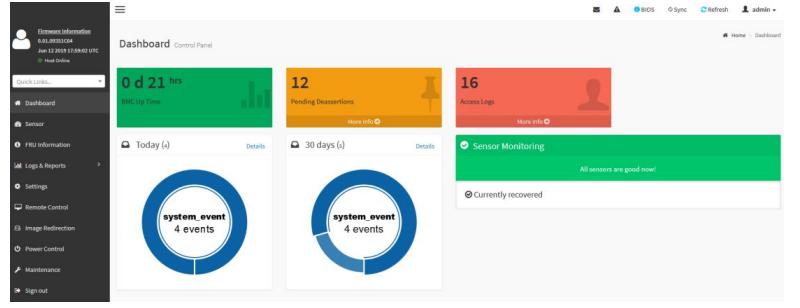
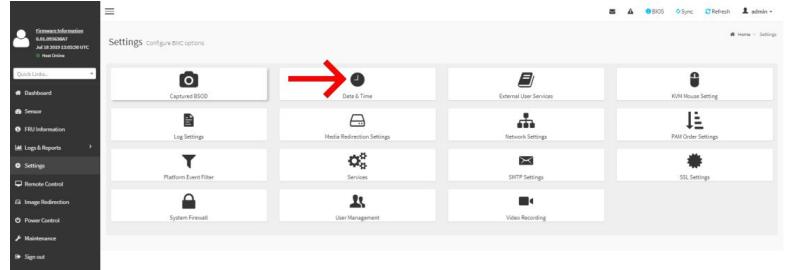
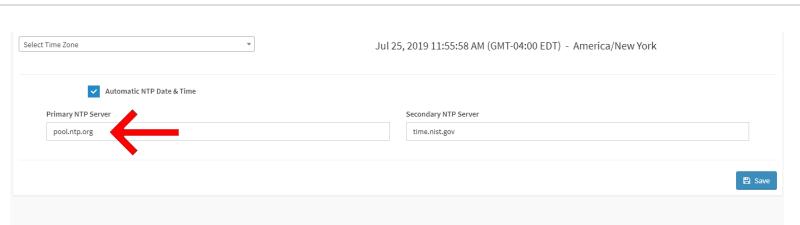
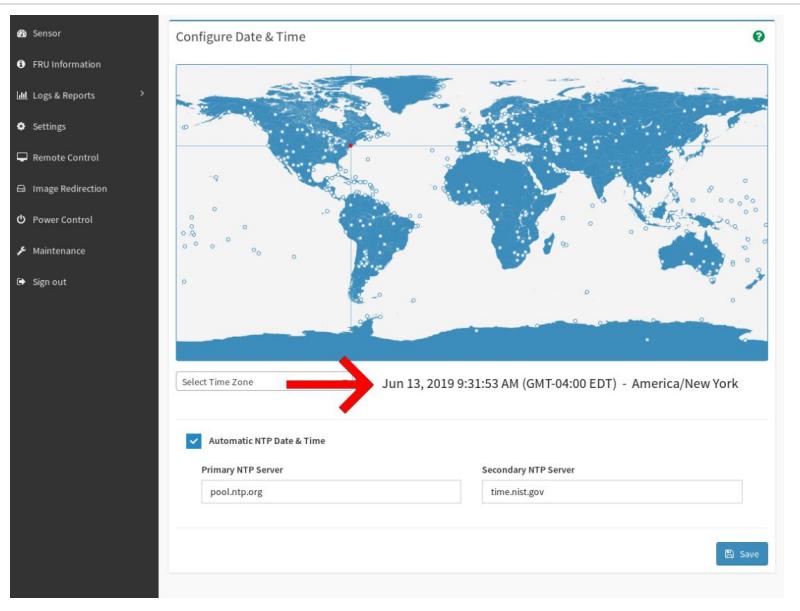
Relevant sections:

[Baseboard management controller - BMC](#)

[Accessing a BMC on an ME1100](#)

### Procedure

## PRELIMINARY

Step_1	<p>From a remote computer that has access to the management network subnet, access the BMC Web UI using the BMC IP address.</p> 
Step_2	<p>Click on <b>Settings</b> from the left side menu. Then, click on <b>Date &amp; Time</b>.</p> 
Step_3	<p>In the <b>Primary NTP Server</b> field, enter the desired NTP server address.</p> 
Step_4	<p>Verify that the time and date displayed matches the local time and date.</p> <p><b>NOTE:</b> It may take several seconds or minutes before the BMC synchronizes the time with the NTP server.</p> 

## Configuring the NTP using IPMI (IOL or KCS)

### Prerequisites (IOL)

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

### Relevant sections:

[Baseboard management controller - BMC](#)

# PRELIMINARY

[Accessing the operating system of a server](#)

## Prerequisites (KCS)

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

Relevant section:

[Accessing the operating system of a server](#)

## Getting the BMC time and date

Step_1	Access the operating system using an IPMI method (IOL or KCS).
Step_2	Verify that the local time and date match the server's time and date.  LocalServer_OSPrompt:~# ipmitool sel time get

## Setting the BMC time and date

Relevant sections:

[Decoding NTP raw configuration data](#)

## PRELIMINARY

## Confirming configuration

Step_1	<p>Get the BMC time and date.</p> <pre>LocalServer_OSPrompt:~# ipmitool sel time get</pre>	<pre>[root@localhost ~]# ipmitool sel time get 07/16/2019 23:14:24</pre>
Step_2	<p>Verify that the BMC time and date match with the local time and date. NOTE: It may take several seconds or minutes before the BMC synchronizes time with the NTP server.</p>	

## Decoding NTP raw configuration data

## PRELIMINARY

Bytes	Description	Possible values
0	Status of NTP	<ul style="list-style-type: none"><li>• 0x00: Disabled</li><li>• 0x01: Enabled</li><li>• 0x02: Failure status</li></ul>
1:128	Primary Server IP, MSB First	Hexadecimal values (0:255)
139:256	Secondary Server IP, MSB First	Hexadecimal values (0:255)

This script can be used to convert string data to raw data and to pad the raw data with the required number of 0.

### Address conversion

```
string=$(printf "10.1.20.10" | od -t d1 | head -n1 | sed 's/00000000 //g' | sed 's/ //g')"  
length=$(echo $string | wc -w)  
  
string_padded="$string"  
for i in $(seq 0 $((127 - length))); do  
    string_padded="$string_padded 0"  
done  
echo $string_padded
```



To convert ascii and hexadecimal data, you can use this online tool  
<https://www.rapidtables.com/convert/number/ascii-to-hex.html> and pad to 128 bytes with 0.

# Basic BIOS option configuration

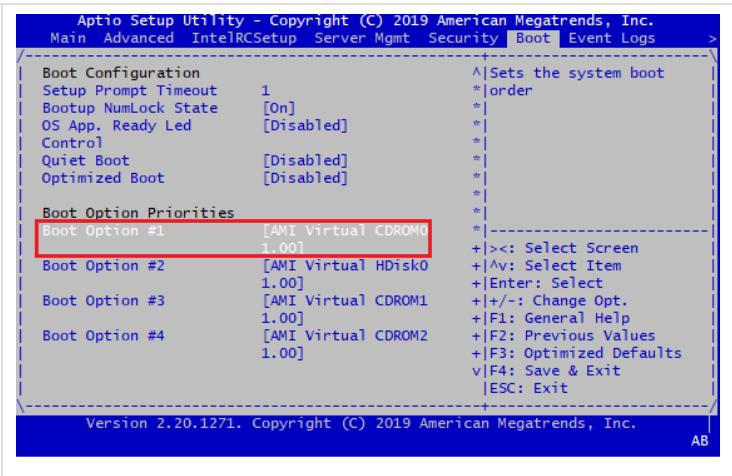
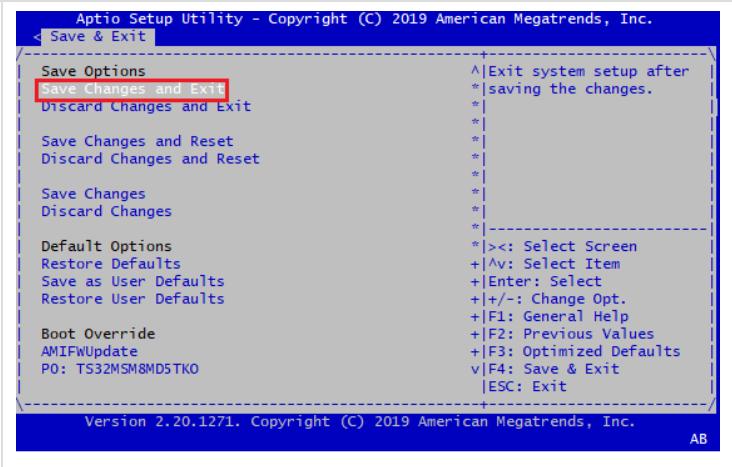
{This section details the most common configuration options related to the BIOS.}

Table of contents

- [Changing the boot order](#)
- [Overriding the boot order](#)
- [Enabling secure boot](#)
- [Configuring the TPM](#)
- [Configuring the BIOS using Redfish](#)
- [Application Ready LED control](#)

## Changing the boot order

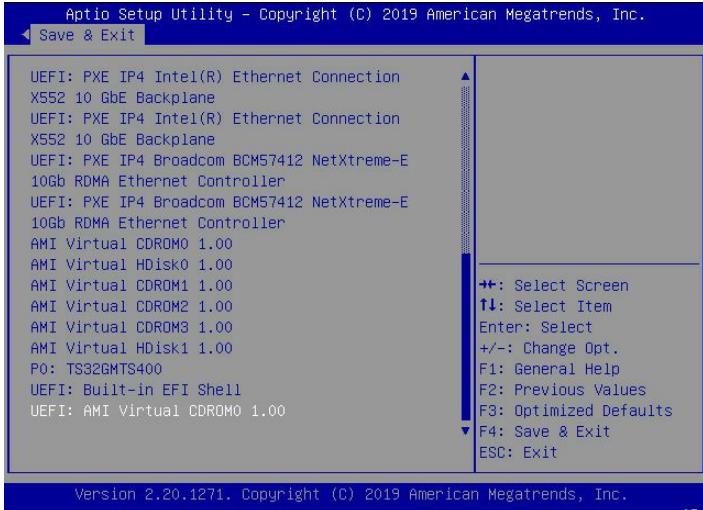
Refer to [Accessing the BIOS](#) for access instructions.

Step_1	<p>From the BIOS setup menu, use the keyboard arrows to select the <b>Boot</b> menu. Configure the boot order as desired.</p>	
Step_2	<p>Using the keyboard arrows, select the <b>Save &amp; Exit</b> menu, go to <b>Save Changes and Exit</b> and press <b>Enter</b> to confirm and save the new boot order.</p>	

## Overriding the boot order

Refer to [Accessing the BIOS](#) for access instructions.

## PRELIMINARY

Step_1	<p>From the BIOS setup menu and using the keyboard arrows, select the <b>Save &amp; Exit</b> menu. In the <b>Boot Override</b> section, select the desired option and press <b>Enter</b>. The server will boot from a particular device.</p> <p><b>NOTE:</b> this selection will only affect the current boot.</p>  <p>The screenshot shows the BIOS setup utility interface. The title bar reads "Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc." and the sub-menu bar says "Save &amp; Exit". The main menu lists various boot options. A vertical help menu on the right side provides key bindings for navigation and function keys F1 through F4. The bottom of the screen displays the version information "Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc." and the letters "AB".</p>
--------	---

## Enabling secure boot

Refer to [Accessing the BIOS](#) for access instructions.

# PRELIMINARY

Step_1	<p>To enable the secure boot option, the CSM module must be disabled.</p> <p>Navigate to Advanced → CSM Configuration</p> <p>Set the CSM Support to [Disabled]</p> <p>Note that all Option ROM execution modes (Network, Storage, Video, other) must be set to [UEFI] before CSM Support can be disabled.</p>	<p>Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Advanced</p> <p>Compatibility Support Module Configuration CSM Support [Disabled]  Enable/Disable CSM Support.</p> <p> &lt;: Select Screen  &gt;: Select Screen  &lt;: Select Item  &gt;: Select Item  Enter: Select  Enter: Select  +/-: Change Opt.  +/-: Change Opt.  F1: General Help  F1: General Help  F2: Previous Values  F2: Previous Values  F3: Optimized Defaults  F3: Optimized Defaults  F4: Save &amp; Exit  F4: Save &amp; Exit  ESC: Exit  ESC: Exit</p> <p>Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</p>
Step_2	Navigate to <b>Save &amp; Exit</b> , then choose <b>Save Changes and Exit</b> .	<p>Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Save &amp; Exit</p> <p>Save Options  Exit system setup after saving the changes. Save Changes and Exit Discard Changes and Exit</p> <p>Save Changes and Reset Discard Changes and Reset</p> <p>Save Changes Discard Changes</p> <p>Default Options Restore Defaults Save as User Defaults Restore User Defaults</p> <p>Boot Override</p> <p> &lt;: Select Screen  &gt;: Select Screen  ^v: Select Item  ^v: Select Item  Enter: Select  Enter: Select  +/-: Change Opt.  +/-: Change Opt.  F1: General Help  F1: General Help  F2: Previous Values  F2: Previous Values  F3: Optimized Defaults  F3: Optimized Defaults  F4: Save &amp; Exit  F4: Save &amp; Exit  ESC: Exit  ESC: Exit</p> <p>Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</p>
Step_3	Return to the BIOS menu by pressing <b>DEL</b> during the boot.	
Step_4	Navigate to the <b>Security</b> option, at the bottom of that menu, go to <b>Secure Boot</b> .	<p>Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IntelRCSetup Server Mgmt Security Boot Event Logs &gt;</p> <p>If ONLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup. If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights. The password length must be in the following range: Minimum length 3 Maximum length 20</p> <p>Administrator Password User Password</p> <p> &gt; Secure Boot</p> <p> &lt;: Select Screen  &gt;: Select Screen  ^v: Select Item  ^v: Select Item  Enter: Select  Enter: Select  +/-: Change Opt.  +/-: Change Opt.  F1: General Help  F1: General Help  F2: Previous Values  F2: Previous Values  F3: Optimized Defaults  F3: Optimized Defaults  F4: Save &amp; Exit  F4: Save &amp; Exit  ESC: Exit  ESC: Exit</p> <p>Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</p>
Step_5	<p>Set the <b>Secure Boot</b> to <b>[Enabled]</b>. Then, if required, you can configure keys using the <b>Secure Boot Mode</b> [<b>Custom</b>].</p>	<p>Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Security</p> <p>System Mode User  Secure Boot feature is Active if Secure Boot is Enabled, Secure Boot [Enabled]  Platform Key(PK) is enrolled and the System is in User mode. Active  The mode change requires platform reset</p> <p>Secure Boot Mode [Standard]</p> <p> &gt; Restore Factory Keys  &gt; Reset To Setup Mode</p> <p> &gt; Key Management</p> <p> &lt;: Select Screen  &gt;: Select Screen  ^v: Select Item  ^v: Select Item  Enter: Select  Enter: Select  +/-: Change Opt.  +/-: Change Opt.  F1: General Help  F1: General Help  F2: Previous Values  F2: Previous Values  F3: Optimized Defaults  F3: Optimized Defaults  F4: Save &amp; Exit  F4: Save &amp; Exit  ESC: Exit  ESC: Exit</p> <p>Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.</p>

## Configuring the TPM

Refer to [Accessing the BIOS](#) for access instructions.

# PRELIMINARY

<p><b>Step_1</b></p> <p>To configure the TPM options. Navigate to Advanced → Trusted Computing</p>	<pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IntelBCSetup Server Mgmt Security Boot Event Logs &gt; &gt; Trusted Computing ^Trusted Computing &gt; ACPI Settings *Settings &gt; Redfish Host Interface Settings * &gt; Serial Port Console Redirection * &gt; PCI Subsystem Settings * &gt; USB Configuration * &gt; CSM Configuration * &gt; NVMe Configuration * &gt; Network Stack Configuration * &gt; iSCSI Configuration + &gt;: Select Screen &gt; Tls Auth Configuration +`v: Select Item &gt; RAM Disk Configuration +Enter: Select &gt; VLAN Configuration (MAC:DA3BC1B62F03) +/+-: Change Opt. &gt; MAC:DA3BC1B62F03-IPv4 Network Configuration +F1: General Help &gt; Intel(R) Ethernet Connection X552 10 GbE SFP+ +F2: Previous Values - 00:AO:A5:D7:FC:DD +F3: Optimized Defaults  +F4: Save &amp; Exit   ESC: Exit  AB Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. </pre>
<p><b>Step_2</b></p> <p>By default, the TPM is enabled. In that menu, you can configure the TPM options according to your needs.</p> <p><b>NOTE:</b> In Linux, the IFX vendor uses Infineon kernel modules.</p>	<pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Advanced TPM20 Device Found Firmware Version: 5.63 ^Enables or Disables Vendor: IFX *BIOS support for Security Device [Enable] * security device. O.S. Support * will not show Security Active PCR banks SHA-1,SHA256 * Device, TCG EFI Available PCR banks SHA-1,SHA256 * protocol and INT1A  * interface will not be  * available.  * SHA-1 PCR Bank [Enabled] * -----* SHA256 PCR Bank [Enabled] *`&gt;: Select Screen  *`v: Select Item  *Enter: Select  */+-: Change Opt.  +F1: General Help  +F2: Previous Values  +F3: Optimized Defaults  +F4: Save &amp; Exit   ESC: Exit  AB Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. </pre> <pre> Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Advanced Active PCR banks SHA-1,SHA256 ^ TPM 1.2 will restrict Available PCR banks SHA-1,SHA256 + support to TPM 1.2  + devices, TPM 2.0 will  + restrict support to TPM  + 2.0 devices, Auto will  + support both with the  + default set to TPM 2.0  + devices if not found,  * Pending operation [None] * -----* Platform Hierarchy [Enabled] *`&gt;: Select Screen Storage Hierarchy [Enabled] *`v: Select Item Endorsement [Enabled] *Enter: Select  */+-: Change Opt.  +F1: General Help  +F2: Previous Values  +F3: Optimized Defaults  +F4: Save &amp; Exit   ESC: Exit  AB Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. </pre>

## Configuring the BIOS using Redfish

Refer to [Accessing the BIOS using Redfish](#) for access instructions.

## PRELIMINARY

Step_1	Access the BIOS menu using Redfish and select the attribute to configure.	<pre>\$ curl -k -s --compressed https://Administrator:superuser@172.16.205.245/redfish/v1/Registers/BiosAttributeRegistry1100_2.21.0.json   jq -r '.RegistryEntries.Attributes[]   .AttributeName , .DisplayName, ""'   grep "Boot" -B 8 SECB001 Secure Boot -- SECB002 Secure Boot Mode -- SETUPO04 Bootup NumLock State -- SETUPO05 Quiet Boot -- SETUPO06 Boot Option Priorities -- GPNV005 Log System Boot Event</pre>
Step_2	Read the value of the configuration to verify if any modification is required. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Systems/Self/Bios   jq '.Attribute. [ATTRIBUTE_TAG]'	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Systems/Self/Bios   jq '.Attributes.SETUPO05' false</pre>
Step_3	Set the value of the BIOS configuration. RemoteComputer_OSPrompt:~\$ curl -k -s -X PUT [ROOT_URL]Systems/Self/Bios/S D -H 'If-None-Match : W/"0"' -H 'Content-Type: application/json' -d '{ "Attributes": { "[ATTRIBUTE_TAG]": "[VALUE]" }}' NOTE: All the BIOS configurations done in Redfish are not instantly changed in the BIOS. The platform needs to be reset in order for the settings to change.	<pre>\$ curl -k -s -X PUT https://Administrator:superuser@172.16.205.245/redfish/v1/Systems/Self/Bios   jq -d '{ "Attributes": { "SETUPO05": true}}'</pre>
Step_4	If necessary, verify the Redifsh BIOS change commands queued in the SD ressource. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Systems/Self/Bios/SD   jq	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Systems/Self/Bios/SD   jq</pre>
Step_5	Perform an ACPI shutdown on the platform. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"GracefulShutdown"}' -H "Content-Type: application/json"	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self/ResetActionInfo   jq {   "odata.context": "/redfish/v1/metadata#ActionInfo",   "odata.etag": "W/\"1563595964\"",   "odata.id": "/redfish/v1/Chassis/Self/ResetActionInfo",   "odata.type": "#ActionInfo.v1_0_3.ActionInfo",   "Description": "This action is used to reset the Chassis",   "Id": "ResetAction",   "Name": "ResetAction",   "Parameters": [     {       "AllowableValues": [         "ForceRestart",         "ForceOff",         "GracefulShutdown"       ],       "Type": "String",       "Name": "ResetType",       "Required": true     }   ] }</pre>
Step_6	Wait for the PowerState to be "Off". RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self   jq .PowerState	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self   jq .PowerState "Off"</pre>
Step_7	Power on the platform. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL ]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"On"}' -H "Content-Type: application/json"	
Step_8	Verify that the setting value changed correctly. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL ]Systems/Self/Bios   jq '.Attribute. [ATTRIBUTE_TAG]'	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Systems/Self/Bios   jq '.Attributes.SETUPO05' true</pre>

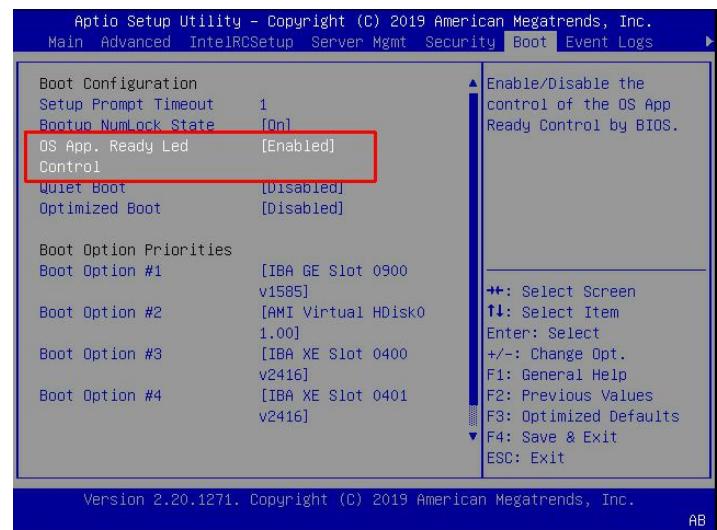
## Application Ready LED control

Note: The Power LED blinks at 50%, 1Hz during platform power-up. It indicates that the application is NOT ready. It can be changed to solid lit either by the BIOS before OS load or by the client's application.

Refer to [Accessing the BIOS](#) for access instructions.

## PRELIMINARY

- Step\_1 From the Boot BIOS setup menu, select the OS App. Ready Led Control option and press Enter to change its value.  
When the option is set to Enabled , the LED will stop blinking just before the BIOS launches the operating system.  
When the option is set to Disabled , the LED will not stop blinking. It will be the responsibility of the client's application to do the necessary action to make it stop. Refer to [Application ready indication via power LED](#).



## Operating

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

Children

- [Default user names and passwords](#)
- [Accessing platform components](#)
- [Platform power management](#)
- [Monitoring](#)
- [Maintenance](#)
- [Platform cooling and thermal management](#)
- [Application ready indication via power LED](#)

## Default user names and passwords

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

Table of contents

- [Operating system](#)
- [BIOS](#)
- [Management interface \(BMC\)](#)

### Operating system

The user name and password are application-specific.

### BIOS

No password is set by default.

### Management interface (BMC)

	The BMC can be accessed using SNMP. However, before configuring SNMP, the default user name and password must be changed as a minimum of 8 characters are required for both. Refer to <a href="#">Configuring BMC user names and passwords using the Web UI</a> .
--	---

The ME1100 platform includes one BMC.

User interface	User name	Password
Web UI	admin	admin
IPMI		
Redfish	Administrator	superuser
SNMP	New 8 character minimum user name configured in the Web UI	New 8 character minimum password configured in the Web UI

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

## Accessing platform components

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

Children

- [Accessing the operating system of a server](#)
- [Accessing the BIOS](#)
- [Accessing a BMC on an ME1100](#)

# 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 Serial over LAN \(SOL\)](#)
  - [Prerequisites](#)
  - [Access procedure](#)
- [Accessing an OS using SSH, RDP or customer application protocols](#)
  - [Prerequisites](#)
  - [Access procedure](#)
- [Accessing an OS using a 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 [Serial over LAN \(SOL\)](#)
- 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

### Prerequisites

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

### Browser considerations

## PRELIMINARY

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

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

### Access procedure

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

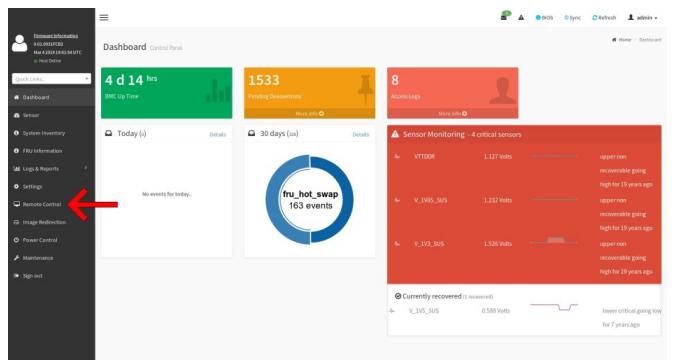
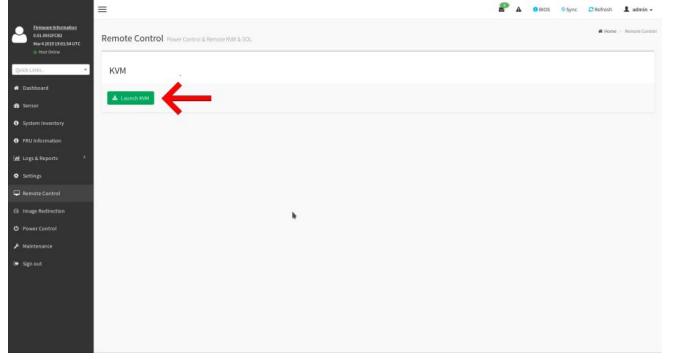
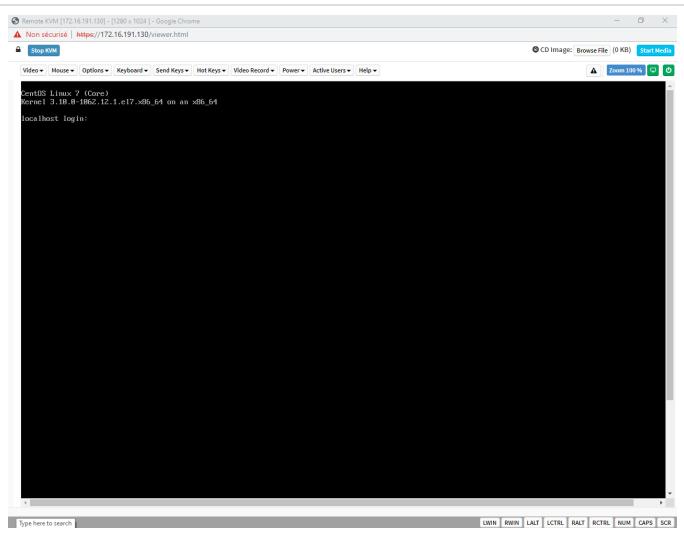
To obtain the list of default user names and passwords, refer to [Default user names and passwords](#).

# PRELIMINARY

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

# PRELIMINARY

## Launching the KVM

Step_1	From the left menu, click on <b>Remote Control</b> .	
Step_2	From the <b>Remote Control</b> menu, click on the <b>Launch KVM</b> button.	
Step_3	A new browser window opens and displays the server screen. <b>NOTE:</b> If an OS is installed, the image displayed might be that of the OS.	

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

## Accessing an OS using Serial over LAN (SOL)

### Prerequisites

1	An OS is installed.
2	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
3	The remote computer has access to the management network subnet.
4	A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

# PRELIMINARY

## Access procedure

To obtain the list of default user names and passwords, refer to [Default user names and passwords.](#)

Step_1	From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name]-P [IPMI password] sol deactivate	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin sol deactivate
Step_2	Activate an SOL session. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name]-P [IPMI password] sol activate	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin sol activate [SOL Session operational. Use ~? for help]  CentOS Linux 7 (Core) Kernel 3.10.0-957.el7.x86_64 on an x86_64  localhost login: root Password: Last login: Thu Jun 27 13:21:19 on ttys0  ***** Kontron installs the bare bone images of the OS distribution and version ordered by the customer. The customer is entirely responsible to configure their OS, to install their applications and to maintain security updates that answer their unique performance and security needs.  Accordingly, Kontron will not be held liable for any problems or any damages caused as a result of not complying with this requirement. Kontron is able to install custom OS that answers your requirement. Contact your Kontron sales representative to learn more about our professional services offer.  We strongly recommend changing the login username "root" and password "kontron" set by Kontron. After acknowledging this disclaimer, it's possible to edit the welcome message by modifying the file /etc/motd ***** [root@localhost ~]#
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.

## Access procedure

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

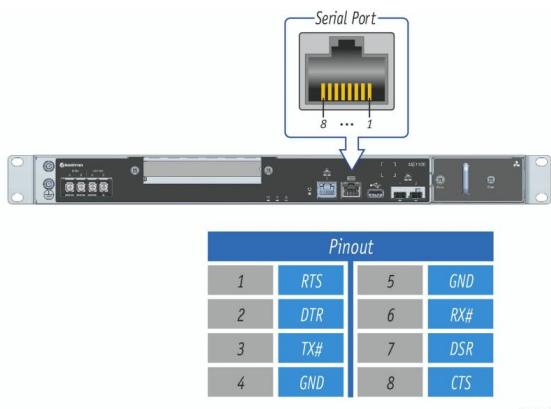
## Accessing an OS using a serial console (physical connection)

# PRELIMINARY

## Prerequisites

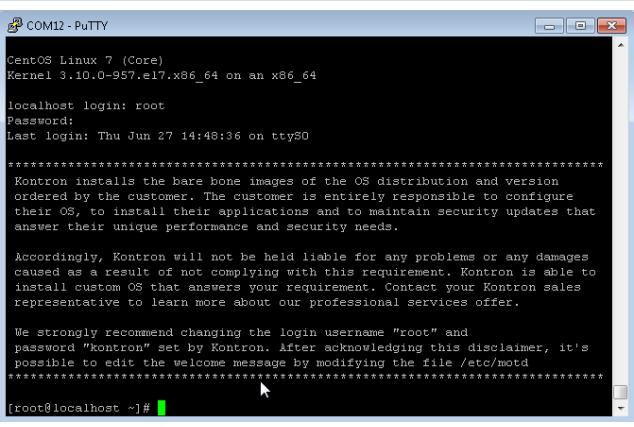
1	An OS is installed.
2	A physical connection to the device is required. NOTE: The serial console port is compatible with Cisco 72-3383-01 cable.
3	A serial console tool is installed on the external computer. <ul style="list-style-type: none"><li>• Speed (Baud): 115200</li><li>• Data bits: 8</li><li>• Stop bits: 1</li><li>• Parity: None</li><li>• Flow Control: None</li><li>• Recommended emulation mode: VT100+</li></ul> 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](#).

Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.
Step_2	The OS start screen will be displayed.  <p>The screenshot shows a black terminal window with white text. At the top, it says 'COM12 - PuTTY'. Below that, the text reads: CentOS Linux 7 (Core) Kernel 3.10.0-957.el7.x86_64 on an x86_64 localhost login: root Password: Last login: Thu Jun 27 14:48:36 on ttys0 ***** Kontron installs the bare bone images of the OS distribution and version ordered by the customer. The customer is entirely responsible to configure their OS, to install their applications and to maintain security updates that answer their unique performance and security needs. Accordingly, Kontron will not be held liable for any problems or any damages caused as a result of not complying with this requirement. Kontron is able to install custom OS that answers your requirement. Contact your Kontron sales representative to learn more about our professional services offer. We strongly recommend changing the login username "root" and password "kontron" set by Kontron. After acknowledging this disclaimer, it's possible to edit the welcome message by modifying the file /etc/motd ***** [root@localhost ~]#</p>

NOTE : If the OS is not displayed, perform a server reset. Refer to [Platform power management](#).

# PRELIMINARY

# Accessing the BIOS

## Table of contents

- [Accessing the BIOS using the KVM](#)
  - [Prerequisites](#)
  - [Browser considerations](#)
  - [Access procedure](#)
    - [Accessing the BMC of the server for which you want to access the BIOS](#)
    - [Launching the KVM](#)
    - [Accessing the BIOS setup menu](#)
- [Accessing the BIOS using Serial over LAN \(SOL\)](#)
  - [Prerequisites](#)
- [Accessing the BIOS using a serial console \(physical connection\)](#)
  - [Prerequisites](#)
  - [Port location](#)
  - [Access procedure](#)
- [Accessing the BIOS using Redfish](#)
  - [Prerequisites](#)
  - [Access procedure](#)

The BIOS can be accessed through various methods:

- Using the [KVM](#) – this is the recommended path for first time out-of-the-box system configuration
- Using [Serial over LAN \(SOL\)](#)
- Using a [serial console \(physical connection\)](#)
- Using [Redfish](#)

Refer to [Description of system access methods](#) for more information on the various paths.

## Accessing the BIOS using the KVM

### Prerequisites

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

### Relevant section:

[Baseboard management controller - BMC](#)

### Browser considerations

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

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

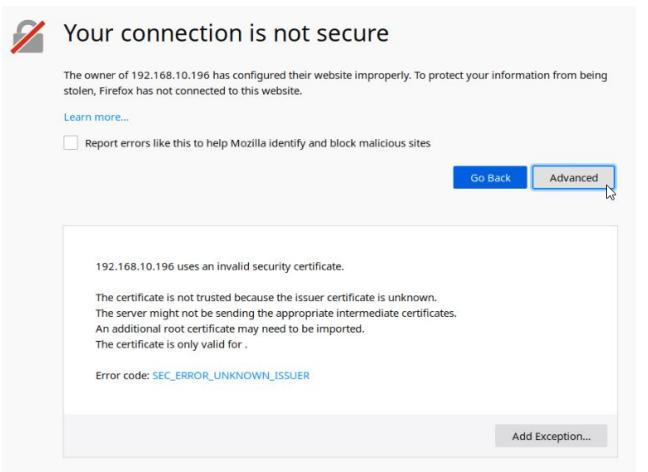
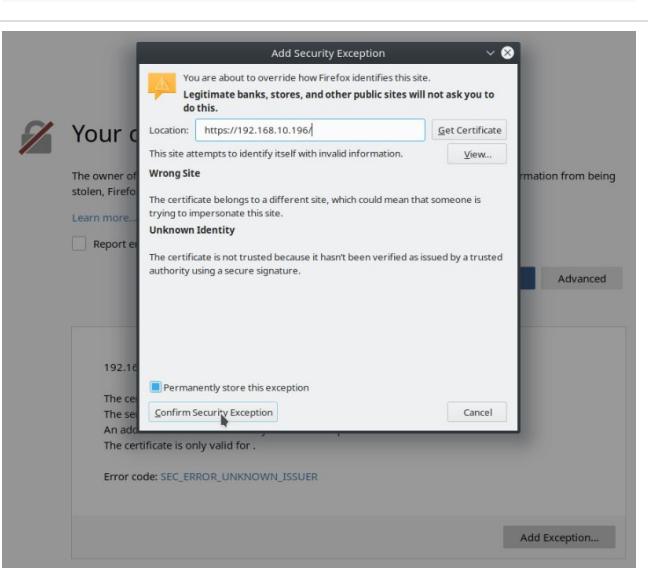
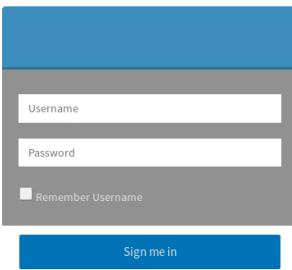
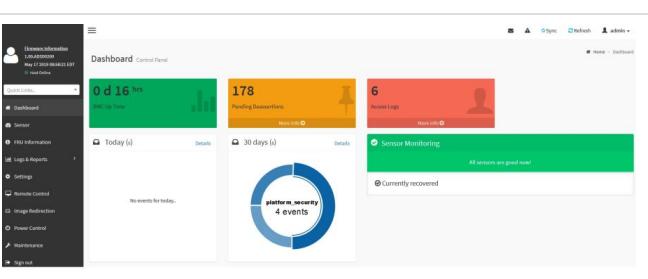
## PRELIMINARY

### Access procedure

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

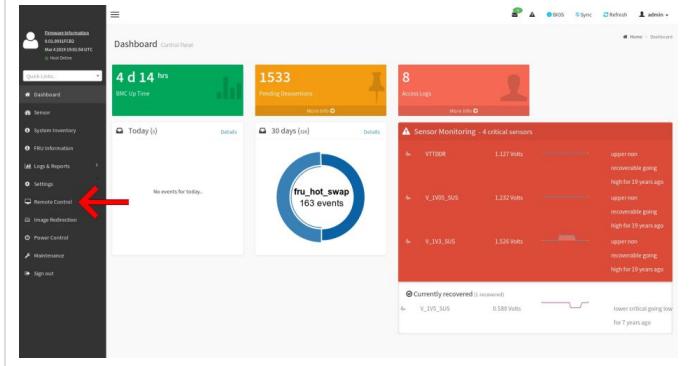
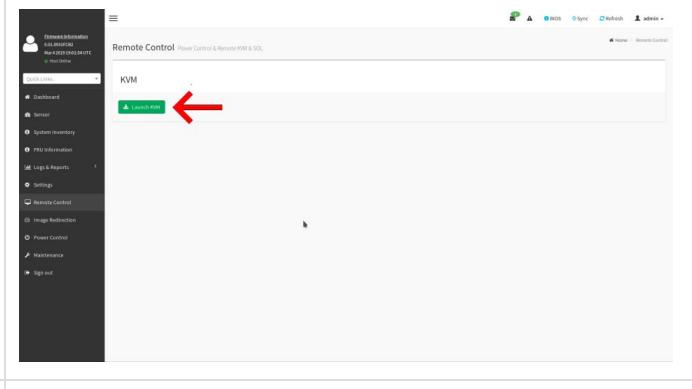
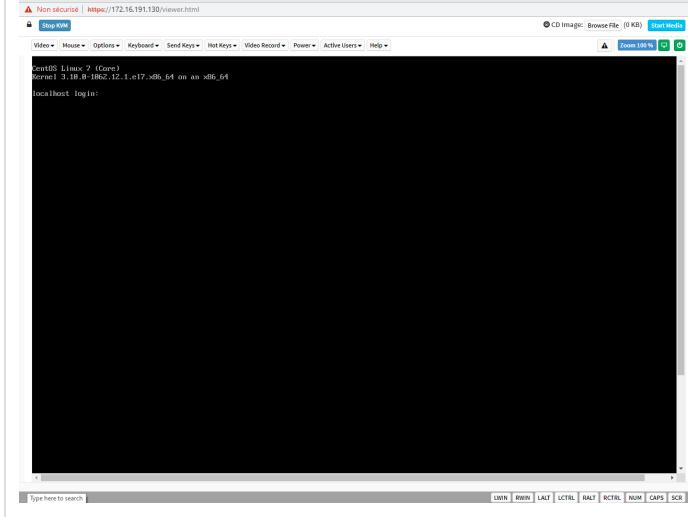
To obtain the list of default user names and passwords, refer to [Default user names and passwords](#).

# PRELIMINARY

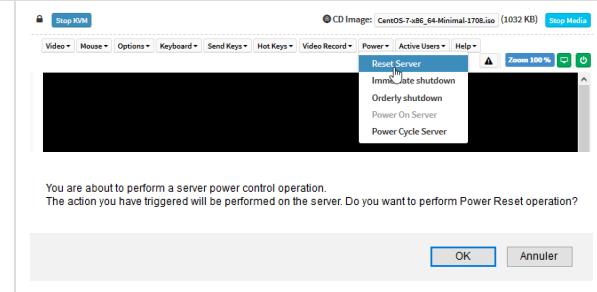
Step_1	<p>From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC.</p> <p><b>NOTE: The HTTPS prefix is mandatory.</b></p> <p><b><a href="https://[BMC MNGMT_IP]">https://[BMC MNGMT_IP]</a></b></p>	
Step_2	<p>Click on <b>Advanced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

# PRELIMINARY

## Launching the KVM

Step_1	From the left menu, click on <b>Remote Control</b> .	
Step_2	From the <b>Remote Control</b> menu, click on the <b>Launch KVM</b> button.	
Step_3	<p>A new browser window opens and displays the server screen.  <b>NOTE:</b> If an OS is installed, the image displayed might be that of the OS.</p>	

## Accessing the BIOS setup menu

Step_1	<p>From the <b>Power</b> drop-down menu, select <b>Reset Server</b> to access the BIOS menu. Click on <b>OK</b> to confirm the operation.  <b>NOTE:</b> When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.</p>	
Step_2	<p>When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.  <b>NOTE:</b> It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup..."</p>	

## PRELIMINARY

### Tip:

Some users are pressing DEL/F2 many times and very rapidly, to make sure the server catches the key and enters the BIOS setup menu. Doing this may lead to following message on the KVM display:

**HID Queue is about to get full. Kindly hold on a second(s)..**

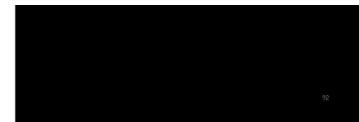
Kontron suggests modifying the **Setup Prompt**

**Timeout** parameter to give users more time to react.

Keeping the focus (single-tasking) on the KVM window is also a good practice to enter the BIOS setup menu each time it is needed.

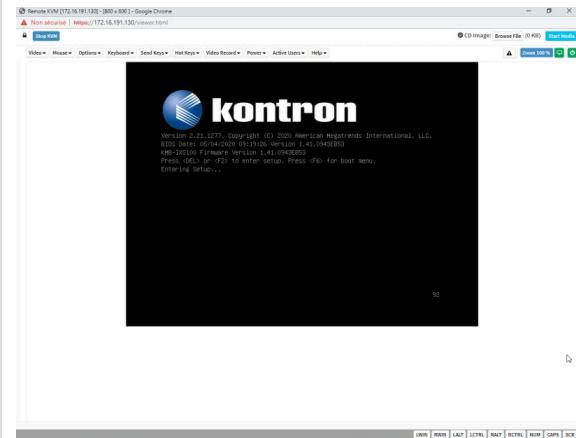
Parameter **Setup Prompt Timeout** is found in the **Boot** tab of the BIOS setup menu.

The default value is 1 second, but changing it to a value between 3 and 10 seconds is a good target range.



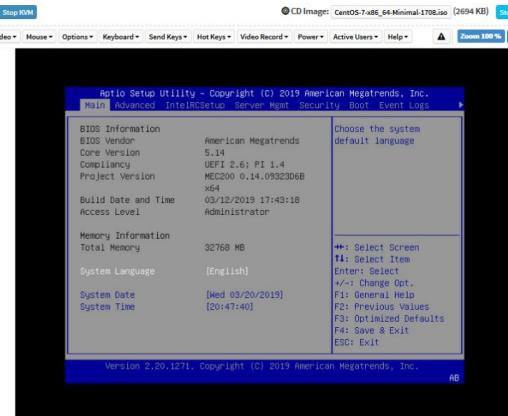
LINH PHEM LAST LCTRL RALT RCTRL NMH CAPS SCR

**Step\_3** The BIOS sign on screen displays "Entering Setup...".  
NOTE: It will take several seconds to display and enter the BIOS setup menu.



LINH PHEM LAST LCTRL RALT RCTRL NMH CAPS SCR

**Step\_4** The BIOS setup menu will be displayed.



## Accessing the BIOS using Serial over LAN (SOL)

### Prerequisites

1	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2	The remote computer has access to the management network subnet.
3	A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

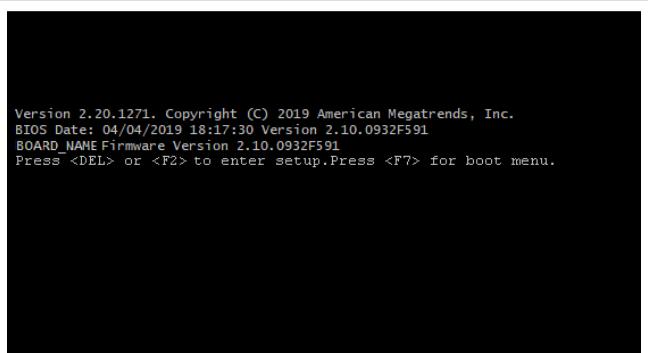
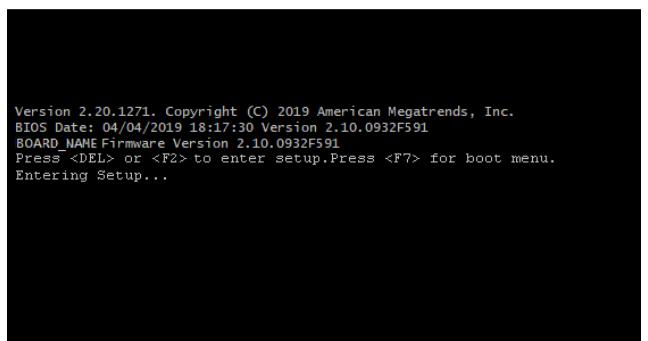
# PRELIMINARY

Relevant section:

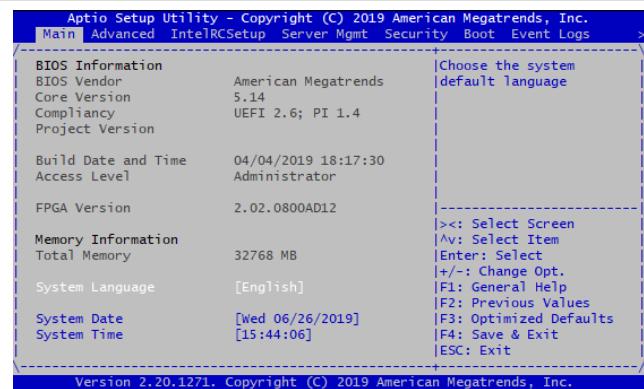
[Baseboard management controller - BMC](#)

## Access procedure

To obtain the list of default user names and passwords, refer to [Default user names and passwords](#).

Step_1	<p>From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sol deactivate</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin sol deactivate</pre>
Step_2	<p>Activate an SOL session.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sol activate</pre> <p><b>NOTE:</b> It may be required to press the <b>Enter</b> key for the operating system's screen to be displayed.</p>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin sol activate [SOL Session operational. Use ~? for help]  CentOS Linux 7 (Core) Kernel 3.10.0-957.el7.x86_64 on an x86_64  localhost login: root Password: Last login: Thu Jun 27 13:21:19 on ttys0 ***** Kontron installs the bare bone images of the OS distribution and version ordered by the customer. The customer is entirely responsible to configure their OS, to install their applications and to maintain security updates that answer their unique performance and security needs.  Accordingly, Kontron will not be held liable for any problems or any damages caused as a result of not complying with this requirement. Kontron is able to install custom OS that answers your requirement. Contact your Kontron sales representative to learn more about our professional services offer.  We strongly recommend changing the login username "root" and password "kontron" set by Kontron. After acknowledging this disclaimer, it's possible to edit the welcome message by modifying the file /etc/motd *****</pre> <p>[root@localhost ~]#  </p>
Step_3	<p>Perform a server reset.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] chassis power reset</pre> <p><b>NOTE:</b> When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.</p>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power reset System Information BOARD_NAME System BIOS Version: 2.10.0932F591 Date: "04/04/2019" Intel RC Version: 02.05.00 CPU Info: Intel(R) Xeon(R) CPU D-1548 @ 2.00GHz Memory Info: Memory Size: 32GB Memory Speed: 2400MHz RAS Mode: Indep 0x32 : CPU POST-Memory Initialization. 0x4F : DXE IPL Start. 0x68 : PCI HB Initialization. 0x70 : SB DXE Initialization. 0x79 : CSM Driver Entry point. 0x91 : Connecting Drivers. 0x92 : PCI Bus Initialization. 0x94 : PCI Bus Enumeration. 0x95 : PCI Bus Request Resources. 0x96 : PCI Bus Assign Resources. 0x91 : Connecting Drivers. 0x92 : PCI Bus Initialization. 0x97 : Console Output devices connect.</pre>
Step_4	<p>When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.</p> <p><b>NOTE:</b> It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup...".</p>	
Step_5	<p>The BIOS sign on screen displays "Entering Setup...".</p> <p><b>NOTE:</b> It will take several seconds to display and enter the BIOS setup menu.</p>	

Step\_6 The BIOS setup menu is displayed.

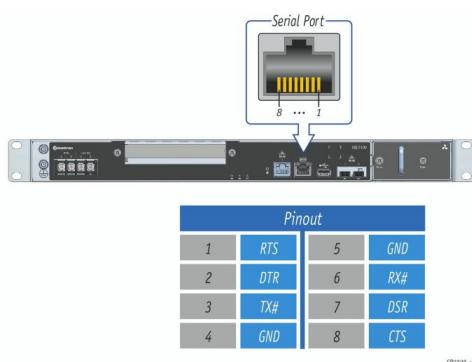


## Accessing the BIOS using a serial console (physical connection)

### Prerequisites

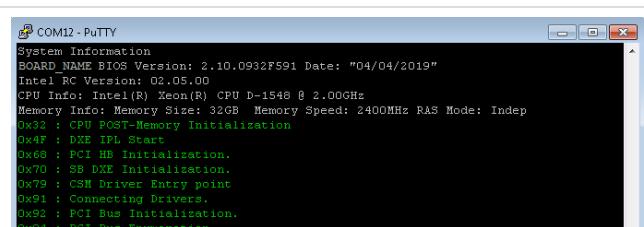
1	A physical connection to the device is required. <b>NOTE:</b> The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the external computer. <ul style="list-style-type: none"> <li>• Speed (Baud): 115200</li> <li>• Data bits: 8</li> <li>• Stop bits: 1</li> <li>• Parity: None</li> <li>• Flow Control: None</li> <li>• Recommended emulation mode: VT100+</li> </ul> <b>NOTE:</b> PuTTY is recommended.

### Port location



### Access procedure

Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.
Step_2	Perform a server reset ( <b>Ctrl-break</b> hot key). <b>NOTE:</b> If an operating system is installed on the device, the hot key might not work properly. If this is the case, reset the server as recommended for the operating system. <b>NOTE:</b> When a server reset command is sent, it

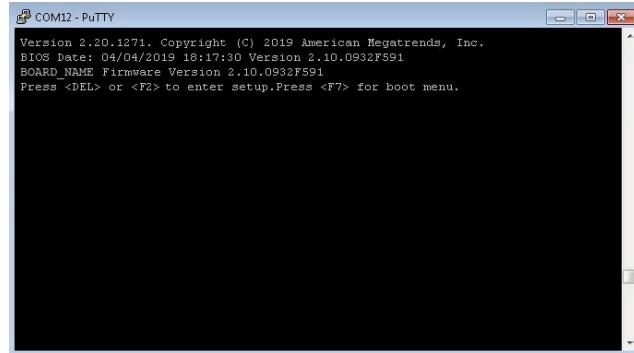


## PRELIMINARY

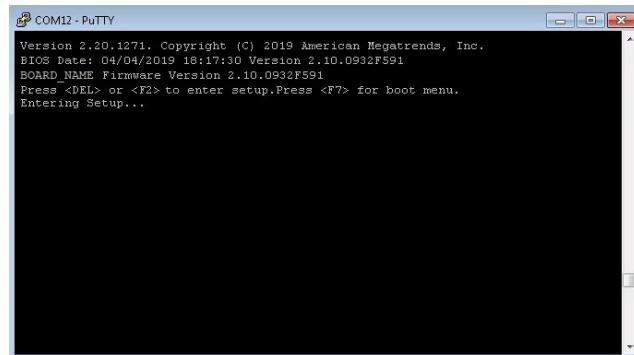
may take a few seconds for the BIOS sign on screen to display.

```
0x94 : PCI Bus Enumeration.
0x95 : PCI Bus Request Resources.
0x96 : PCI Bus Assign Resources.
0x91 : Connecting Drivers.
0x92 : PCI Bus Initialization.
0x97 : Console Output devices connect.
```

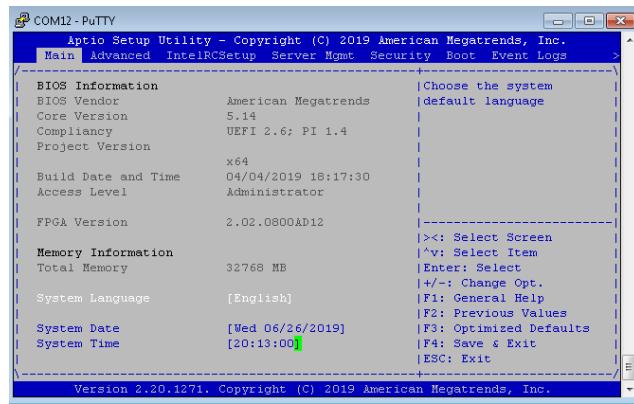
- Step\_3** When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.  
**NOTE:** It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup...".



- Step\_4** The BIOS sign on screen displays "Entering Setup...".  
**NOTE:** It will take several seconds to display and enter the BIOS setup menu.



- Step\_5** The BIOS setup menu is displayed.



## Accessing the BIOS using Redfish

### Prerequisites

1	The Redfish root URL is known (refer to Configuring/Configuring system access methods).
2	An HTTP client tool is installed on the remote computer.
3	A JSON parser command-line tool such as jq is installed.

### Access procedure

## PRELIMINARY

Step_1	<p>Find the Redfish BiosAttributeRegistry and its version number by using this command:</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL] Registries   jq   grep BiosAttribute</pre> <p><b>NOTE:</b> This version changes when the BIOS gets updated.</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.206.10/redfish/v1/Registries   jq   grep BiosAttribute   "@odata.id": "/redfish/v1/Registries/BiosAttributeRegistry1100..2.21.0"</pre>
Step_2	<p>Access the following Redfish ressource. It describes all the available BIOS configurations and their possible values.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s --compressed [ROOT_URL]Registries/[BIOS_REGISTRY].json   jq</pre>	<pre>\$ curl -k -s --compressed https://Administrator:superuser@172.16.205.245/redfish/v1/Registries/BiosAttributeRegistry1100..2.21.0.json   jq {   "@odata.type": "#AttributeRegistry.v1_2_0.AttributeRegistry",   "Description": "This registry defines a representation of BIOS Attribute instances",   "Id": "BiosAttributeRegistry1100..2.21.0",   "Language": "en-US",   "Name": "I100_BIOS_Attribute_Registry",   "OwningEntity": "AMT",   "RegistryVersion": "2.21.0",   "odata.context": "/redfish/v1/\$metadata#AttributeRegistry.AttributeRegistry",   "odata.etag": "Dummymetag",   "odata.id": "/redfish/v1/Registries/BiosAttributeRegistry1100..2.21.0.json",   "RegistryEntries": {     "Attributes": [       {         "AttributeName": "TCG003",         "DisplayName": "Security Device Support",         "HelpText": "Enables or Disables BIOS support for security device. O.S. will not show Security Device, TCG EFI protocol and INT1A interface will not be available.",         "ReadOnly": false,         "Type": "Enumeration",         "Value": [           ...         ]       }     ]   } }</pre>
Step_3	<p>Find the attribute tag associated with the desired BIOS configuration by using the following jq filter. It parses the printed list and returns only the attribute tag followed by its description.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s --compressed [ROOT_URL]Registries/[BIOS_REGISTRY].json   jq -r '.RegistryEntries.Attributes[]   .AttributeName , .DisplayName, ""'</pre>	<pre>\$ curl -k -s --compressed https://Administrator:superuser@172.16.205.245/redfish/v1/Registries/BiosAttributeRegistry1100..2.21.0.json   jq -r '.RegistryEntries.Attributes[]   .AttributeName , .DisplayName, ""' TCG003   Security Device Support ACPI004   Enable ACPI Auto Configuration ACPI002   Enable Hibernation ACPI003   Lock Legacy Resources REDF001   Authentication mode REDF002   IP address</pre>
Step_4	<p>(Optional) The use of grep is recommended to locate a specific BIOS configuration in the list. This command prints out the list of settings that contain the search word.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s --compressed [ROOT_URL]Registries/[BIOS_REGISTRY].json   jq -r '.RegistryEntries.Attributes[]   .AttributeName , .DisplayName, ""'   grep "[WORD]" -B 1</pre>	<pre>\$ curl -k -s --compressed https://Administrator:superuser@172.16.205.245/redfish/v1/Registries/BiosAttributeRegistry1100..2.21.0.json   jq -r '.RegistryEntries.Attributes[]   .AttributeName , .DisplayName, ""'   grep "Boot" -B 1 SEC8001   Secure Boot   --   SEC8002   Secure Boot Mode   --   SETUP004   Bootup NumLock State   --   SETUP005   Quiet Boot   --   SETUP006   Boot Option Priorities   --   GPNV005   Log System Boot Event</pre>
Step_5	<p>Read the configuration value.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL ]Systems/Self/Bios   jq '.Attribute.[ATTRIBUTE_TAG] '</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Systems/Self/Bios   jq '.Attributes.SETUP005' false</pre>

# Accessing a BMC on an ME1100

## Table of contents

- [Accessing a BMC using the Web UI](#)
  - [Prerequisites](#)
  - [Browser considerations](#)
  - [Access procedure](#)
- [Accessing a BMC using IPMI over LAN \(IOL\)](#)
  - [Prerequisites](#)
  - [Access procedure](#)
- [Accessing a BMC using IPMI via KCS](#)
  - [Prerequisites](#)
  - [Access procedure](#)
- [Accessing a BMC using Redfish](#)
  - [Prerequisites](#)
  - [Access procedure](#)
- [Accessing a BMC using BMC SNMP](#)
  - [Prerequisites](#)
  - [Access procedure](#)

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 [IPMI over LAN \(IOL\)](#)
- Using [IPMI via KCS](#)
- Using [Redfish](#)
- Using [BMC SNMP](#)

Refer to [Description of system access methods](#) for more information on the various paths.

## Accessing a BMC using the Web UI

### Prerequisites

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

### Relevant section:

[Baseboard management controller - BMC](#)

### Browser considerations

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

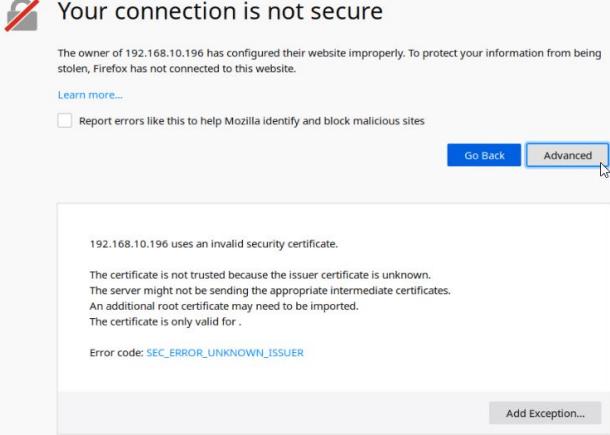
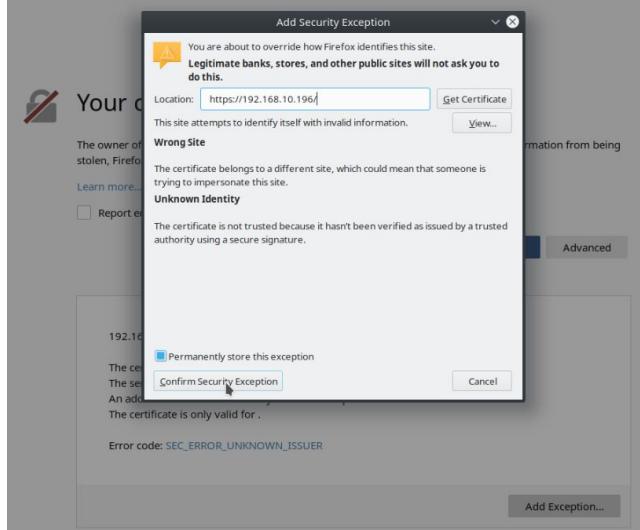
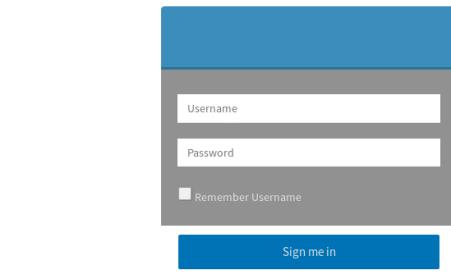
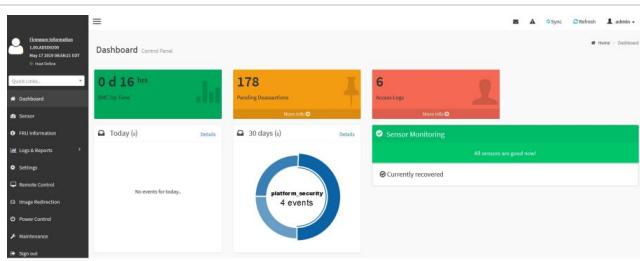
## **PRELIMINARY**

**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.](#)

# PRELIMINARY

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

# Accessing a BMC using IPMI over LAN (IOL)

## Prerequisites

1	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2	The remote computer has access to the management network subnet.
3	A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

### Relevant section:

[Baseboard management controller - BMC](#)

## Access procedure

To obtain the list of default user names and passwords, refer to [Default user names and passwords](#).

Step_1	<p>From a remote computer that has access to the management network subnet, enter the desired command.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] [IPMI command]</pre>	<pre>ipmitool -I lanplus -H 172.16.205.245 -U admin -P admin sensor Temp CPU   46,000   degrees C   ok   0,000 CPU Status   0x0   discrete   0x0080  na Temp DIMM A   30,000   degrees C   ok   0,000 Temp DIMM B   33,000   degrees C   ok   0,000 FRU0 Hot Swap   0x0   discrete   0x1080  na Temp Inlet   26,000   degrees C   ok   0,000 Temp BMC   41,000   degrees C   ok   0,000 Temp Vcore   44,000   degrees C   ok   0,000 Temp Cortina   41,000   degrees C   ok   0,000</pre>
--------	--	---

For a list of supported IPMI commands, refer to [Supported IPMI commands](#).

For a list of all the sensors, refer to [Sensor list](#).

# Accessing a BMC using IPMI via KCS

## Prerequisites

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

## Access procedure

Step_1	<p>From a remote computer that has access the server OS through SSH, RDP or the platform serial port, enter the desired command.</p> <pre>LocalServer_OSPrompt:~# ipmitool [IPMI command]</pre>	<pre>ipmitool sensor Temp CPU   46,000   degrees C   ok   0,000 CPU Status   0x0   discrete   0x0080  na Temp DIMM A   30,000   degrees C   ok   0,000 Temp DIMM B   33,000   degrees C   ok   0,000 FRU0 Hot Swap   0x0   discrete   0x1080  na Temp Inlet   26,000   degrees C   ok   0,000 Temp BMC   41,000   degrees C   ok   0,000 Temp Vcore   44,000   degrees C   ok   0,000 Temp Cortina   41,000   degrees C   ok   0,000</pre>
--------	---	--

For a list of supported IPMI commands, refer to [Supported IPMI commands](#).

For a list of all the sensors, refer to [Sensor list](#).

# Accessing a BMC using Redfish

## Prerequisites

1	The Redfish root URL is known (refer to Configuring/Configuring system access methods).
2	An HTTP client tool is installed on the remote computer.
3	A JSON parser command-line tool such as jq is installed.

### Relevant section:

[Configuring system access methods](#)

## Access procedure

Step_1	Access the Redfish API using the root URL. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]   jq	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/   jq {   "@odata.context": "/redfish/v1/\$metadata#ServiceRoot.ServiceRoot",   "@odata.etag": "W/\"1563378044\"",   "@odata.id": "/redfish/v1/",   "@odata.type": "#ServiceRoot.v1_2_0.ServiceRoot",   "AccountService": {     "@odata.id": "/redfish/v1/AccountService"   },   "Chassis": {     "@odata.id": "/redfish/v1/Chassis"   },   "CompositionService": {     "@odata.id": "/redfish/v1/CompositionService"   },   "Description": "The service root for all Redfish requests on this host",   "EventService": {     "@odata.id": "/redfish/v1/EventService"   },   "Id": "RootService",   "JsonSchemas": {     "@odata.id": "/redfish/v1/JsonSchemas"   }, }</pre>
Step_2	Add the Managers/Self extension. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL] Managers/Self   jq	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Managers/Self   jq {   "@odata.context": "/redfish/v1/\$metadata#Manager.Manager",   "@odata.etag": "W/\"1563378044\"",   "@odata.id": "/redfish/v1/Managers/Self",   "@odata.type": "#Manager.v1_3_1.Manager",   "Actions": {     "#Manager.Reset": {       "ResetType@Redfish.AllowableValues": [         "ForceRestart"       ],       "target": "/redfish/v1/Managers/Self/Actions/Manager.Reset"     },     "#Manager.FactoryReset": {       "FactoryResetType@Redfish.AllowableValues": [         "ResetAll"       ],       "target": "/redfish/v1/Managers/Self/Actions/Manager.FactoryReset"     }   },   "Oem": {     "#Manager.FactoryReset": {       "FactoryResetType@Redfish.AllowableValues": [         "ResetAll"       ],       "target": "/redfish/v1/Managers/Self/Actions/Manager.FactoryReset"     }   } },</pre>

# Accessing a BMC using BMC SNMP

NOTE : The current implementation supports version 3 of the SNMP protocol. For the commands to work, snmpwalk version 5.8 or higher must be installed.

# PRELIMINARY

## Prerequisites

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

### Relevant sections:

[Configuring system access methods](#)

[Baseboard management controller - BMC](#)

## Access procedure

Step_1	From a remote computer that has access to the management network subnet, enter the desired command. RemoteComputer_OSPrompt:~# snmpwalk -v 3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [BMC MNGMT_IP] [OID]	\$ snmpwalk -v 3 -l authPriv -u snmpaccess -a SHA-256 -A snmppassword -x DES -X snmppassword 172.16.192.250 SNMPv2-SMI::enterprises.15000.554.2.1.1.0 = STRING: "ME1100_00A0A5D63E9C" SNMPv2-SMI::enterprises.15000.554.2.1.1.1 = INTEGER: 1 SNMPv2-SMI::enterprises.15000.554.2.1.1.2 = INTEGER: 2 SNMPv2-SMI::enterprises.15000.554.2.1.1.3 = INTEGER: 3 SNMPv2-SMI::enterprises.15000.554.2.1.1.4 = INTEGER: 4 SNMPv2-SMI::enterprises.15000.554.2.1.1.5 = INTEGER: 5 SNMPv2-SMI::enterprises.15000.554.2.1.1.6 = INTEGER: 6 SNMPv2-SMI::enterprises.15000.554.2.1.1.7 = INTEGER: 7 SNMPv2-SMI::enterprises.15000.554.2.1.1.8 = INTEGER: 8 SNMPv2-SMI::enterprises.15000.554.2.1.1.9 = INTEGER: 9
--------	--	--

# Platform power management

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

Table of contents

- [Available power commands](#)
- [Power off](#)
- [Power on](#)
- [Reset \(warm boot\)](#)
- [Power cycle \(cold boot\)](#)
- [ACPI shutdown \(clean shutdown\)](#)
- [Sending a power command using the Web UI](#)

## Available power commands

The power states of the ME1100 platform can be managed using various commands sent through the platform Web UI or an IPMI client (IOL or KCS).

It is recommended to use the Web UI, and automation of power management tasks requires an IPMI access.

The power commands are:

- [Power off](#): Immediately powers off the platform. **WARNING** : This command does not initiate a clean shutdown of the operating system prior to powering down the system.
- [Power on](#): Powers on the platform.
- [Reset \(warm boot\)](#): Reboots the platform without turning off power. **WARNING** : This command does not initiate a clean shutdown of the operating system prior to rebooting the system.
- [Power cycle \(cold boot\)](#): Powers off the platform before rebooting it. **WARNING** : This command does not initiate a clean shutdown of the operating system prior to rebooting the system.
- [ACPI shutdown \(clean shutdown\)](#): Initiates and completes the operating system's shutdown prior to powering off the platform. **NOTE**: ACPI must be supported by the server's operating system.

## Power off

- Using the [Web UI](#)
- Using [IPMI \(IOL\)](#)
- Using [IPMI \(KCS\)](#)
- Using [Redfish](#)

### Power off using IPMI (IOL)

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

## PRELIMINARY

Step_1	<p>From a remote computer that has access to the management network subnet, open the OS command prompt and power off the platform.</p> <p>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power off</p>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power off Chassis Power Control: Down/Off</pre>
Step_2	<p>Verify the power status to confirm the power action has succeeded.</p> <p>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power status</p>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status Chassis Power is off</pre>

### Power off using IPMI (KCS)

Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

Step_1	<p>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, power off the platform.</p> <p>LocalServer_OSPrompt:~# ipmitool chassis power off</p>	<pre>[root@localhost ~]# ipmitool chassis power off Chassis Power Control: Down/Off [root@localhost ~]# [ OK ] Started Show Plymouth Power Off Screen. [ OK ] Stopped Login Service. [ OK ] Started Restore /run/initramfs. [ OK ] Stopped Dynamic System Tuning Daemon. [ OK ] Stopped target Network.       Stopping Network Manager... [ OK ] Stopped Network Manager.       Stopping D-Bus System Message Bus... [ OK ] Stopped D-Bus System Message Bus. [ OK ] Stopped target Basic System. [ OK ] Stopped target Slices. [ 1713.778354] systemd-shutdown[1]: Successfully changed into root pivot. [ 1713.785578] systemd-shutdown[1]: Returning to initrd... [ 1713.868933] dracut Warning: Killing all remaining processes dracut Warning: Killing all remaining processes [ 1713.941615] XFS (dm-0): Unmounting Filesystem [ 1713.950789] dracut Warning: Unmounted /oldroot. [ 1713.988380] dracut: Disassembling device-mapper devices [ 1714.023424] kvm: exiting hardware virtualization Powering off. [ 1714.030097] sd 0:0:0:0: [sda] Synchronizing SCSI cache [ 1714.035282] sd 0:0:0:0: [sda] Stopping disk [ 1714.126569] pcieport 0000:00:1c.4: System wakeup enabled by ACPI [ 1715.159367] ACPI: Preparing to enter system sleep state S5 [ 1715.165354] Power down.</pre>
--------	--	--

### Power off using Redfish

Refer to [Accessing a BMC using Redfish](#) for access instructions.

## PRELIMINARY

<p><b>Step_1</b></p> <p>Print the list of available power actions.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self/ResetActionInfo   jq</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/chassis/Self/ResetActionInfo   jq {   "odata.context": "#redfish.v1.SObjectType.ActionInfo.ActionInfo",   "odata.etag": "\"\$\"15d55519464\"\"",   "odata.id": "/redfish/v1/Chassis/Self/ResetActionInfo",   "odata.type": "#ActionInfo.v1_0_3.ActionInfo",   "Description": "This action is used to reset the Chassis",   "Name": "ResetAction",   "Parameters": [     {       "AllowableValues": [         "ForceRestart",         "ForceOff",         "On",         "GracefulShutdown"       ],       "DataType": "String",       "Name": "ResetType",       "Required": true     }   ] }</pre>
<p><b>Step_2</b></p> <p>Power off the platform.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"ForceOff"}' -H "Content-Type: application/json"</pre>	
<p><b>Step_3</b></p> <p>Verify the power status.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self   jq .PowerState</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/chassis/Self   jq .PowerState "off"</pre>

## Power on

- Using the [Web UI](#)
- Using [IPMI \(IOL\)](#)
- Using [Redfish](#)

### Power on using IPMI (IOL)

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

<p><b>Step_1</b></p> <p>From a remote computer that has access to the management network subnet, open the OS command prompt and power on the platform.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC_MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power on</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power on Chassis Power Control: Up/On</pre>
<p><b>Step_2</b></p> <p>Verify the power status to confirm the power action has succeeded.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC_MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power status</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status Chassis Power is on</pre>

### Power on using Redfish

Refer to [Accessing a BMC using Redfish](#) for access instructions.

## PRELIMINARY

Step_1	Print the list of available power actions. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL] Chassis/Self/ResetActionInfo   jq	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self/ResetActionInfo   jq {   "@odata.context": "/redfish/v1/\$metadata#ActionInfo.ActionInfo",   "@odata.etag": "W/\"1563559464\"",   "@odata.id": "/redfish/v1/Chassis/Self/ResetActionInfo",   "@odata.type": "#ActionInfo.v1_0_3.ActionInfo",   "Description": "This action is used to reset the Chassis",   "Id": "ResetAction",   "Name": "ResetAction",   "Parameters": [     {       "AllowableValues": [         "ForceRestart",         "ForceOff",         "On",         "GracefulShutdown"       ],       "DataType": "String",       "Name": "ResetType",       "Required": true     }   ] }</pre>
Step_2	Power on the platform. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"On"}' -H "Content-Type: application/json"	
Step_3	Verify the power status. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self   jq .PowerState	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self   jq .PowerState "On"</pre>

## Reset (warm boot)

- Using the [Web UI](#)
- Using [IPMI \(IOL\)](#)
- Using [IPMI \(KCS\)](#)
- Using [Redfish](#)

### Reset (warm boot) using IPMI (IOL)

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

Step_1	From a remote computer that has access to the management network subnet, open the OS command prompt and reset the platform. RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC_MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power reset	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power reset Chassis Power Control: Reset</pre>
Step_2	Verify the power status to confirm the power action has succeeded. RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC_MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power status NOTE: It may take a moment for the OS to reboot.	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status Chassis Power is on</pre>

### Reset (warm boot) using IPMI (KCS)

Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

## PRELIMINARY

<p><b>Step_1</b></p> <p>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, reset the platform.</p> <pre>LocalServer_OSPrompt:~# ipmitool chassis power reset</pre> <p>NOTE: It may take a moment for the OS to reboot.</p>	<pre>[root@localhost ~]# ipmitool chassis power reset Chassis Power Control: Reset</pre>
---	--

### Reset (warm boot) using Redfish

Refer to [Accessing a BMC using Redfish](#) for access instructions.

<p><b>Step_1</b></p> <p>Print the list of available power actions.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL] Chassis/Self/ResetActionInfo   jq</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self/ResetActionInfo   jq {   "@odata.context": "/redfish/v1/\$metadata#ActionInfo.ActionInfo",   "@odata.etag": "W/\"1563559464\"",   "@odata.id": "/redfish/v1/Chassis/Self/ResetActionInfo",   "@odata.type": "#ActionInfo.v1_0_3.ActionInfo",   "Description": "This action is used to reset the Chassis",   "Id": "ResetAction",   "Name": "ResetAction",   "Parameters": [     {       "AllowableValues": [         "ForceRestart",         "ForceOff",         "On",         "GracefulShutdown"       ],       "DataType": "String",       "Name": "ResetType",       "Required": true     }   ] }</pre>
<p><b>Step_2</b></p> <p>Reset the platform.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"ForceRestart"}' -H "Content-Type: application/json"</pre>	
<p><b>Step_3</b></p> <p>Verify the power status.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self   jq .PowerState</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self   jq .PowerState "On"</pre>

### Power cycle (cold boot)

- Using the [Web UI](#)
- Using [IPMI \(IOL\)](#)
- Using [IPMI \(KCS\)](#)

#### Power cycle (cold boot) using IPMI (IOL)

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

## PRELIMINARY

Step_1	<p>From a remote computer that has access to the management network subnet, open the OS command prompt and perform a power cycle.</p> <p>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power cycle</p>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power cycle Chassis Power Control: Cycle</pre>
Step_2	<p>Verify the power status to confirm the power action has succeeded.</p> <p>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power status</p> <p>NOTE: It may take a moment for the OS to reboot.</p>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status Chassis Power is on</pre>

### Power cycle (cold boot) using IPMI (KCS)

Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

Step_1	<p>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, perform a power cycle.</p> <p>LocalServer_OSPrompt:~# ipmitool chassis power cycle</p> <p>NOTE: It may take a moment for the OS to reboot.</p>	<pre>[root@localhost ~]# ipmitool chassis power cycle Chassis Power Control: Cycle</pre>
--------	---	--

### ACPI shutdown (clean shutdown)

- Using the [Web UI](#)
- Using [IPMI \(IOL\)](#)
- Using [IPMI \(KCS\)](#)
- Using [Redfish](#)

### ACPI shutdown using IPMI (IOL)

Refer to [Accessing a BMC using IPMI over LAN \(IOL\)](#) for access instructions.

## PRELIMINARY

Step_1	<p>From a remote computer that has access to the management network subnet, open the OS command prompt and perform an ACPI shutdown.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power soft</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power soft Chassis Power Control: Soft</pre>
Step_2	<p>Verify the power status to confirm the power action has succeeded.</p> <pre>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power status</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status Chassis Power is off</pre>

### ACPI shutdown using IPMI (KCS)

Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

Step_1	<p>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, perform an ACPI shutdown.</p> <pre>LocalServer_OSPrompt:~# ipmitool chassis power soft</pre>	<pre>[root@localhost ~]# ipmitool chassis power soft Chassis Power Control: Soft [root@localhost ~]# [ OK ] Started Show Plymouth Power Off Screen. [ OK ] Stopped Network Manager.           Stopping D-Bus System Message Bus... [ OK ] Stopped D-Bus System Message Bus. [ OK ] Stopped Login Service. [ OK ] Stopped target Basic System.</pre>
--------	---	---

### ACPI shutdown using Redfish

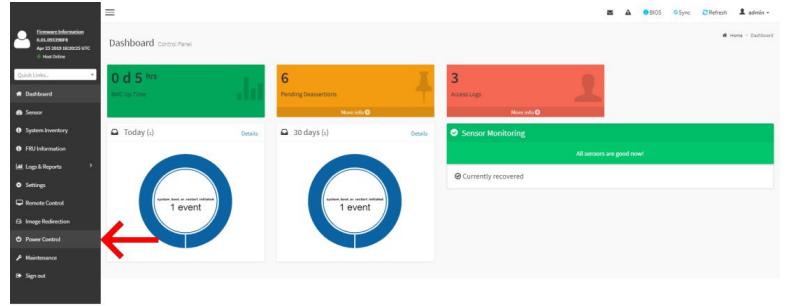
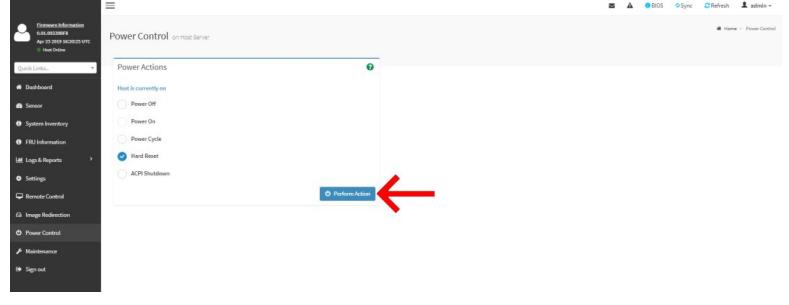
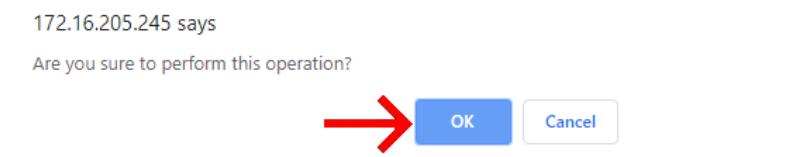
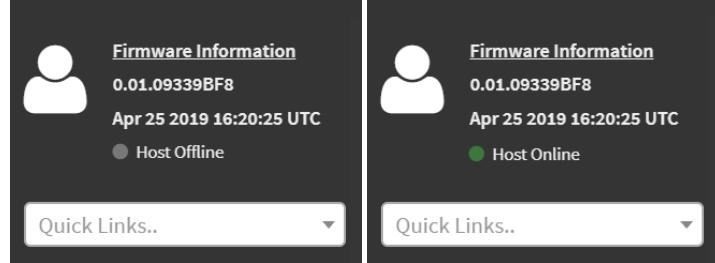
Refer to [Accessing a BMC using Redfish](#) for access instructions.

Step_1	<p>Print the list of available power actions.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self/ResetActionInfo   jq</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self/ResetActionInfo   jq {   "@odata.context": "/redfish/v1/\$metadata#ActionInfo.ActionInfo",   "@odata.etag": "W/\"1563559464\"",   "@odata.id": "/redfish/v1/Chassis/Self/ResetActionInfo",   "@odata.type": "#ActionInfo.v1_0_3.ActionInfo",   "Description": "This action is used to reset the Chassis",   "Id": "ResetAction",   "Name": "ResetAction",   "Parameters": [     {       "AllowableValues": [         "ForceRestart",         "ForceOff",         "On",         "GracefulShutdown"       ],       "DataType": "String",       "Name": "ResetType",       "Required": true     }   ] }</pre>
Step_2	<p>Perform the power action on the platform.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"GracefulShutdown"}' -H "Content-Type: application/json"</pre>	
Step_3	<p>Verify the power status.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self   jq .PowerState</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self   jq .PowerState "on"</pre>

### Sending a power command using the Web UI

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

# PRELIMINARY

Step_1	Access the BMC Web UI of a server.	
Step_2	Once you are logged into the Web UI, click on Power Control from the left side menu.	
Step_3	Select the desired power action. Press on the Perform Action button.	
Step_4	A confirmation prompt will appear. Confirm the action by clicking on OK. Upon confirmation, the selected action will be performed and the platform status will be updated after a few minutes.	
Step_5	Verify the power status by looking at the power status in the left side menu.	

## Monitoring

Children

- [Monitoring sensors](#)
- [Sensor list](#)
- [Interpreting sensor data](#)
- [Managing customer added sensors](#)

## Monitoring sensors

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

Table of contents

- [Monitoring using the BMC Web UI](#)
  - [Accessing sensor details](#)
  - [Configuring sensors](#)
- [Monitoring using IPMI](#)
  - [Viewing sensor details](#)
  - [Configuring sensors](#)
- [Monitoring using Redfish](#)
  - [Creating URL extensions](#)
  - [Viewing sensor details](#)
- [Monitoring using BMC SNMP](#)
  - [Viewing the sensor list](#)
  - [Viewing sensor details](#)

The platform has many sensors, you can refer to the [Sensor list](#) for details and to determine the sensor ID.

There are several methods to monitor platform sensors, including:

- Using the [BMC Web UI](#)
- Using [IPMI](#)
- Using [Redfish](#)
- Using [BMC SNMP](#)

For sensor data interpretation instructions, refer to [Interpreting sensor data](#).

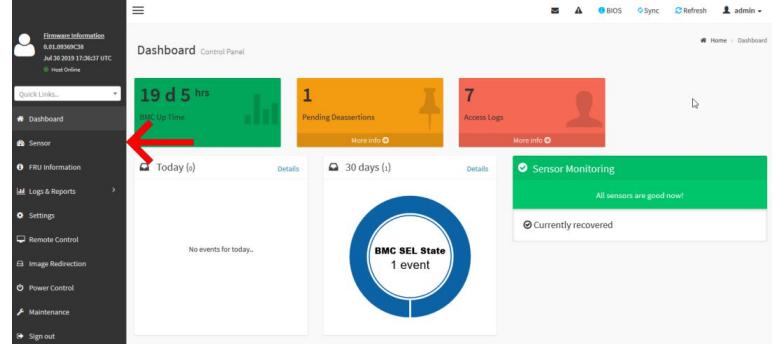
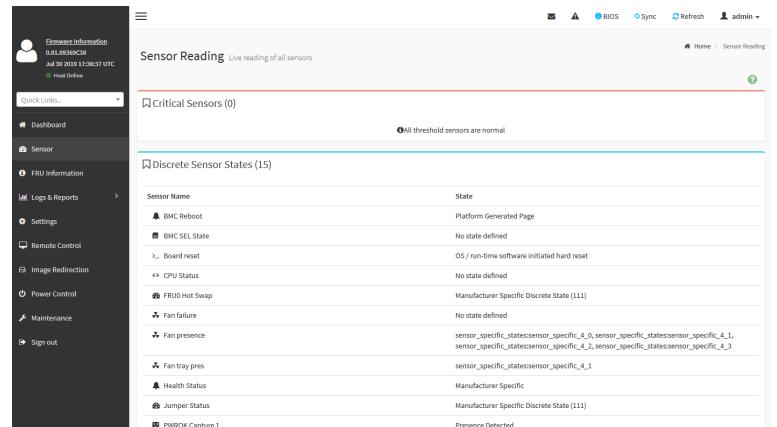
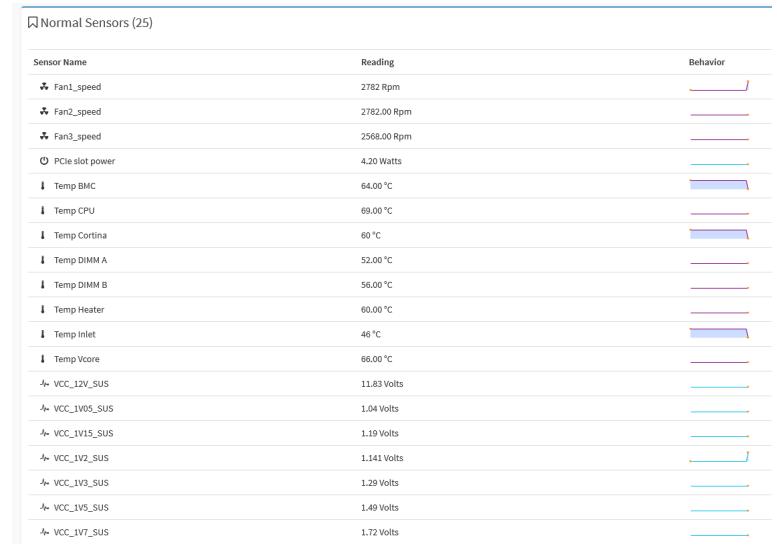
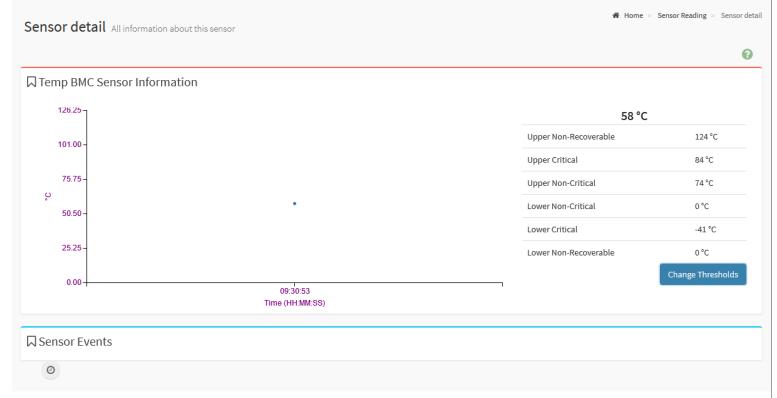
For instructions on how to access the BMC, refer to [Accessing a BMC on an ME1100](#).

## Monitoring using the BMC Web UI

### Accessing sensor details

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

# PRELIMINARY

Step_1	Access the BMC Web UI.
Step_2	From the left-side menu, click on <b>Sensor</b> .
	 <p>A screenshot of the BMC Web UI Dashboard. On the left, a sidebar menu includes 'Sensor' under 'Logs &amp; Reports'. The main dashboard shows '19 d 5 hrs' of BMC Up Time, 1 pending assertions, and 7 Access Logs. A large circular icon indicates 'BMC SEL State' with 1 event. A red arrow points to the 'Sensor' link in the sidebar.</p>
Step_3	The sensor list will be displayed.
	 <p>A screenshot of the BMC Web UI Sensor Reading page. The sidebar menu again shows 'Sensor'. The main content area displays a table of discrete sensor states, each with a status icon, name, state, and description. For example, 'BMC SEL State' is listed as 'Platform Generated Page'.</p>
Step_4	Scroll down to see the list of sensors.
	 <p>A screenshot of the BMC Web UI Sensor Reading page, showing a detailed list of 25 normal sensors. Each row includes the sensor name, reading value, and behavior graph. Sensors listed include Fan speeds, temperatures (Temp BMC, Temp CPU, Temp Cortina, Temp DIMM A, Temp DIMM B, Temp Heater, Temp Inlet, Temp Vcore), and various voltage levels (VCC_12V_SUS, VCC_1V05_SUS, VCC_1V15_SUS, VCC_1V2_SUS, VCC_1V4_SUS, VCC_1V6_SUS, VCC_1V7_SUS).</p>
Step_5	Click on a sensor to see more details.
	 <p>A screenshot of the BMC Web UI Sensor detail page for the 'Temp BMC' sensor. It shows a graph of temperature over time, current values (58 °C), and threshold settings. The graph shows a sharp increase from 25.25 to 101.00 at 09:30:53. The right side of the page lists temperature thresholds: Upper Non-Recoverable (124 °C), Upper Critical (84 °C), Upper Non-Critical (74 °C), Lower Non-Critical (0 °C), Lower Critical (-41 °C), and Lower Non-Recoverable (0 °C). A 'Change Thresholds' button is visible.</p>

## Configuring sensors

## PRELIMINARY

**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.

<p>Step_1</p> <p>From the sensor detail page, click on <b>Change Thresholds</b>.</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="text-align: right; padding-right: 10px;">58 °C</th> </tr> </thead> <tbody> <tr> <td>Upper Non-Recoverable</td> <td>124 °C</td> </tr> <tr> <td>Upper Critical</td> <td>84 °C</td> </tr> <tr> <td>Upper Non-Critical</td> <td>74 °C</td> </tr> <tr> <td>Lower Non-Critical</td> <td>0 °C</td> </tr> <tr> <td>Lower Critical</td> <td>-41 °C</td> </tr> <tr> <td>Lower Non-Recoverable</td> <td>-50 °C</td> </tr> </tbody> </table> <p style="text-align: right;"><b>Change Thresholds</b></p>	58 °C		Upper Non-Recoverable	124 °C	Upper Critical	84 °C	Upper Non-Critical	74 °C	Lower Non-Critical	0 °C	Lower Critical	-41 °C	Lower Non-Recoverable	-50 °C
58 °C															
Upper Non-Recoverable	124 °C														
Upper Critical	84 °C														
Upper Non-Critical	74 °C														
Lower Non-Critical	0 °C														
Lower Critical	-41 °C														
Lower Non-Recoverable	-50 °C														
<p>Step_2</p> <p>Set the thresholds as desired and click on <b>Save</b>. Optional: Check <b>Retain Threshold Values</b> if you wish to keep the set thresholds after a BMC reboot</p>	<p>Change Threshold Values</p> <p>Sensor Name: Temp CPU</p> <p>Upper Non-recoverable: 124</p> <p>Upper Critical: 99</p> <p>Upper Non-critical: 70</p> <p>Lower Non-critical: NA</p> <p>Lower Critical: -1</p> <p>Lower Non-recoverable: NA</p> <p><input checked="" type="checkbox"/> Retain Threshold Values</p> <p style="text-align: right;"><b>Save</b></p>														

## Monitoring using IPMI

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

### Viewing sensor details

## PRELIMINARY

<p><b>Step_1</b></p> <p>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, enter the command.</p> <pre>LocalServer_OSPrompt:~# ipmitool sensor</pre>	<pre>ipmitool sensor Temp CPU            46,000      degrees C   ok       0,000 CPU Status          0x0         discrete     0x0080   na Temp DIMM A         30,000      degrees C   ok       0,000 Temp DIMM B         33,000      degrees C   ok       0,000 FRU0 Hot Swap      0x0         discrete     0x1080   na Temp Inlet           26,000      degrees C   ok       0,000 Temp BMC            41,000      degrees C   ok       0,000 Temp Vcore           44,000      degrees C   ok       0,000 Temp Cortina         41,000      degrees C   ok       0,000</pre>
<p><b>Step_2</b></p> <p>Use the <code>sdr</code> command to see more details about a specific sensor.</p> <pre>LocalServer_OSPrompt:~# ipmitool sdr get [SENSOR_ID]</pre>	<pre>\$ ipmitool sdr get Fan3_speed Sensor ID          : Fan3_speed (0x2f) Entity ID          : 29.0 (Fan Device) Sensor Type (Threshold) : Fan (0x04) Sensor Reading      : 0 (+/- 0) RPM Status              : ok Nominal Reading     : 856,000 Normal Minimum      : 1712,000 Normal Maximum      : 23005,000 Positive Hysteresis : 535,000 Negative Hysteresis : 535,000 Minimum sensor range : Unspecified Maximum sensor range : Unspecified Event Message Control : Per-threshold Readable Thresholds  : Settable Thresholds  : Assertion Events    : Assertions Enabled   :</pre>

### Configuring sensors

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

<p><b>Step_1</b></p> <p>Change the threshold value of the desired sensor.</p> <pre>LocalServer_OSPrompt:~# ipmitool sensor thresh [SENSOR_ID] [THRESH_TYPE] [VALUE]</pre> <p><b>NOTE:</b> For a negative threshold value add double dashes (--) before the sensor command and type the negative value.</p> <pre>LocalServer_OSPrompt:~# ipmitool -- sensor thresh [SENSOR_ID] [THRESH_TYPE] [NEG VALUE]</pre>	<pre>\$ ipmitool sensor thresh "Temp BMC" unr 180 Locating sensor record 'Temp BMC'... Setting sensor "Temp BMC" Upper Non-Recoverable threshold to 180,000</pre>
---	---

## Monitoring using Redfish

### Creating URL extensions

Type	Sensors	URL extensions
Power sensor	<ul style="list-style-type: none"> <li>• All sensors of type 02h (Voltage)</li> </ul>	<b>Chassis/Self/Power   jq</b>
Thermal	<ul style="list-style-type: none"> <li>• All sensors of type 01h (Temperature)</li> </ul>	<b>Chassis/Self/Thermal   jq ".Temperatures"</b>
	<ul style="list-style-type: none"> <li>• Fan1_speed</li> <li>• Fan2_speed</li> <li>• Fan3_speed</li> <li>• Fan4_speed</li> </ul>	<b>Chassis/Self/Thermal   jq ".Fans"</b>
Health	<ul style="list-style-type: none"> <li>• CPU Status</li> </ul>	<b>Managers/Self/HostInterfaces/Self   jq ".Status"</b>
	<ul style="list-style-type: none"> <li>• Health Status</li> </ul>	<b>Chassis/Self   jq ".Status"</b>

# PRELIMINARY

## Viewing sensor details

Refer to [Accessing a BMC using Redfish](#) for access instructions.

Step_1	<p>Append the root URL with the appropriate extension depending on the type of sensor. Refer to the URL extensions table above.</p> <p>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL][URL_EXTENSION]</p>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self/Power   jq . {   "@odata.context": "/redfish/v1/\$metadata#Power.Power",   "@odata.etag": "W/\"1565102960\"",   "@odata.id": "/redfish/v1/Chassis/Self/Power",   "@odata.type": "#Power.v1_3_0.Power",   "Description": "Power sensor readings",   "Id": "Power",   "Name": "Power",   "PowerControl": [     {       "@odata.id": "/redfish/v1/Chassis/Self/Power#/PowerControl/0",       "MemberId": "ChassisPowerControl0",       "Name": "Chassis Power Control",       "PhysicalContext": "Intake",       "PowerLimit": {         "CorrectionInMs": 1000,         "LimitException": "HardPowerOff",         "LimitInWatts": 500       },       "PowerMetrics": {         "AverageConsumedWatts": 0,         "IntervalInMin": 0,         "MaxConsumedWatts": 0,         "MinConsumedWatts": 0       },       "RelatedItem": {         "@odata.count": 0       }     }   ] }</pre>
--------	---	--

## Monitoring using BMC SNMP

NOTE : The current implementation supports version 3 of the SNMP protocol. For the commands to work, snmpwalk version 5.8 or higher must be installed.

Refer to [Accessing a BMC using BMC SNMP](#) for access instructions.

## Viewing the sensor list

Step_1	<p>To access all the sensors of the BMC, use the following command.</p> <p>RemoteComputer_OSPrompt:~# snmpwalk -v3 -l [AUTH_LEVEL] -a [AUTH_PROTOCOL] -A [PASSWORD] -u [USER_NAME] -x [ENC_PROTOCOL] -X [PASSWORD] [MGMT_IP] SNMPv2-SMI::enterprises.15000.554</p>	<pre>\$ snmpwalk -v 3 -l authPriv -u snmpaccess -a SHA-256 -A snmppassword -x DES -X snmppassword 172.16.192.250 SNMPv2-SMI::enterprises.15000.554 SNMPv2-SMI::enterprises.15000.554.1.0 = STRING: "ME1100_00A0A5D63E9C" SNMPv2-SMI::enterprises.15000.554.2.1.1.1 = INTEGER: 1 SNMPv2-SMI::enterprises.15000.554.2.1.1.2 = INTEGER: 2 SNMPv2-SMI::enterprises.15000.554.2.1.1.3 = INTEGER: 3 SNMPv2-SMI::enterprises.15000.554.2.1.1.4 = INTEGER: 4 SNMPv2-SMI::enterprises.15000.554.2.1.1.5 = INTEGER: 5 SNMPv2-SMI::enterprises.15000.554.2.1.1.6 = INTEGER: 6 SNMPv2-SMI::enterprises.15000.554.2.1.1.7 = INTEGER: 7 SNMPv2-SMI::enterprises.15000.554.2.1.1.8 = INTEGER: 8 SNMPv2-SMI::enterprises.15000.554.2.1.1.9 = INTEGER: 9</pre>
--------	--	---

## Viewing sensor details

Step_1	<p>Print the sensor list. Retrieve the sensor SNMP ID by looking at the last number of the OID.</p> <p>RemoteComputer_OSPrompt:~# snmpwalk -v3 -l [AUTH_LEVEL] -a [AUTH_PROTOCOL] -A [PASSWORD] -u [USER_NAME] -x [ENC_PROTOCOL] -X [PASSWORD] [MGMT_IP] SNMPv2-SMI::enterprises.15000.554.2.1.2</p>	<pre>\$ snmpwalk -v 3 -l authPriv -u snmpaccess -a SHA-256 -A snmppassword -x DES -X snmppassword 172.16.192.250 SNMPv2-SMI::enterprises.15000.554.2.1.2 SNMPv2-SMI::enterprises.15000.554.2.1.2.1 = STRING: "Temp_Inlet" SNMPv2-SMI::enterprises.15000.554.2.1.2.2 = STRING: "Temp_BMC" SNMPv2-SMI::enterprises.15000.554.2.1.2.3 = STRING: "Temp_Vcore" SNMPv2-SMI::enterprises.15000.554.2.1.2.4 = STRING: "Temp_10GbE_PHY" SNMPv2-SMI::enterprises.15000.554.2.1.2.5 = STRING: "Temp_CPU" SNMPv2-SMI::enterprises.15000.554.2.1.2.6 = STRING: "Temp_DIMM_A" SNMPv2-SMI::enterprises.15000.554.2.1.2.7 = STRING: "Temp_DIMM_B" SNMPv2-SMI::enterprises.15000.554.2.1.2.8 = STRING: "Board_Reset" SNMPv2-SMI::enterprises.15000.554.2.1.2.9 = STRING: "PWRok_Capture_1" SNMPv2-SMI::enterprises.15000.554.2.1.2.10 = STRING: "PWRok_Capture_2" SNMPv2-SMI::enterprises.15000.554.2.1.2.11 = STRING: "Health_Status" SNMPv2-SMI::enterprises.15000.554.2.1.2.12 = STRING: "VCC_1V8_LAN" SNMPv2-SMI::enterprises.15000.554.2.1.2.13 = STRING: "V_VPP_DDR" SNMPv2-SMI::enterprises.15000.554.2.1.2.14 = STRING: "V_VTT_DDR" SNMPv2-SMI::enterprises.15000.554.2.1.2.15 = STRING: "V_VDDQ_DDR" SNMPv2-SMI::enterprises.15000.554.2.1.2.16 = STRING: "VCC_1V05_SUS" SNMPv2-SMI::enterprises.15000.554.2.1.2.17 = STRING: "VCC_1V3_SUS" SNMPv2-SMI::enterprises.15000.554.2.1.2.18 = STRING: "VCC_1V7_SUS" SNMPv2-SMI::enterprises.15000.554.2.1.2.19 = STRING: "VCC_3V3_SUS"</pre>
Step_2	<p>Get the value of the sensor.</p> <p>RemoteComputer_OSPrompt:~# snmpget -v3 -l [AUTH_LEVEL] -a [AUTH_PROTOCOL] -A [PASSWORD] -u [USER_NAME] -x [ENC_PROTOCOL] -X [PASSWORD] [MGMT_IP] SNMPv2-SMI::enterprises.15000.554.2.1.3. [SENSOR_ID]</p>	<pre>\$ snmpget -v 3 -l authPriv -u snmpaccess -a SHA-256 -A snmppassword -x DES -X snmppassword 172.16.192.250 SNMPv2-SMI::enterprises.15000.554.2.1.3.12 = INTEGER: 21</pre>

# PRELIMINARY

## Sensor list

*{This article details all sensors of the platform's module.}*

For information about Sensor type code and Event/Reading type code , refer to [Interpreting sensor data](#).

Sensor name [Sensor_ID]	Sensor type code	Event/Reading type code	SNMP sensor number	Description	Implementation notes
Temp CPU	01h(Temperature)	01h(Threshold Based)	5	CPU Temperature	
CPU Status	07h (Processor)	6Fh (Sensor Specific)	45	Processor Status	
Temp DIMM A	01h(Temperature)	01h(Threshold Based)	6	DIMM A0 Temperature via SPD	
Temp DIMM B	01h(Temperature)	01h(Threshold Based)	7	DIMM B0 Temperature via SPD	
Temp Inlet	01h(Temperature)	01h(Threshold Based)	1	Server inlet temperature	
Temp BMC	01h(Temperature)	01h(Threshold Based)	2	BMC Temperature	
Temp Vcore	01h(Temperature)	01h(Threshold Based)	3	Vcore temperature	
Temp 10GbE PHY	01h(Temperature)	01h(Threshold Based)	4	10GbE PHY (SFP+) temperature	
Board reset	1Dh (System Boot/Restart Initiated)	6Fh(Sensor Specific)	8	Board reset type and sources	
PWROK Capture 1	08h (Power Supply)	6Fh(Sensor Specific)	9	Latched power rail status	
PWROK Capture 2	08h (Power Supply)	6Fh(Sensor Specific)	10	Latched power rail status	
V_5V_SUS	02h(Voltage)	01h(Threshold Based)	24	Voltage on board - 5V suspend power supply	
V_12V_SUS	02h(Voltage)	01h(Threshold Based)	23	Voltage on board - 12V suspend power supply	
V_1V8_LAN	02h(Voltage)	01h(Threshold Based)	12	Voltage on board - 1.8V LAN power supply	
V_VPP DDR	02h(Voltage)	01h(Threshold Based)	13	Voltage on board - VppDDR power supply	
V_VTT DDR	02h(Voltage)	01h(Threshold Based)	14	Voltage on board - VttDDR	

PRELIMINARY				
		Based)		vttDDDR power supply
V_VDDQ DDR	02h(Voltage)	01h(Threshold Based)	15	Voltage on board - Vddq power supply
VCC_1V05_SUS	02h(Voltage)	01h(Threshold Based)	16	Voltage on board - 1.05V suspend power supply
VCC_1V15_SUS	02h(Voltage)	01h(Threshold Based)	22	Voltage on board - 1.15V suspend power supply
VCC_1V2_SUS	02h(Voltage)	01h(Threshold Based)	21	Voltage on board - 1.2V suspend power supply
VCC_1V5_SUS	02h(Voltage)	01h(Threshold Based)	20	Voltage on board - 1.5V suspend power supply
VCC_3V3_SUS	02h(Voltage)	01h(Threshold Based)	19	Voltage on board - 3.3V suspend power supply
VCC_1V3_SUS	02h(Voltage)	01h(Threshold Based)	17	Voltage on board - 1.3V suspend power supply
VCC_1V7_SUS	02h(Voltage)	01h(Threshold Based)	18	Voltage on board - 1.7V suspend power supply
Health status	24h(Platform Alert)	7Fh(OEM Health Severity Status Sensor)	11	Overall health status
Ver Change FPGA	2Bh(Version Change)	6Fh(Sensor Specific)	25	FPGA Firmware Change Detection
Ver Change BIOS	2Bh(Version Change)	6Fh(Sensor Specific)	26	BIOS Firmware Change Detection
Ver Change BMC	2Bh(Version Change)	6Fh(Sensor Specific)	27	BMC Firmware Change Detection
Temp NTC	01h(Temperature)	01h(Threshold Based)	28	Thermistor probe placed by customer on the PCIe board Requires the NTC thermistor to be installed by the customer.
BMC Reboot	24h(Platform Alert)	03h ('digital' Discrete - Assert/Deassert)	31	BMC Reboot detection
Jumper Status	D3h (OEM Jumper Status)	6Fh (Sensor Specific)	32	Reflects on-board jumper presence
BMC SEL State	10h(Event Logging Disable)	6Fh (Sensor Specific)	30	Specify the status of the SEL (Cleared/Almost full/Full)
Fan1_speed	04h (Fan)	01h(Threshold Based)	33	Speed of fan #1 (RPM)

## PRELIMINARY

Fan2_speed	04h (Fan)	01h(Threshold Based)	34	Speed of fan #2 (RPM)	
Fan3_speed	04h (Fan)	01h(Threshold Based)	35	Speed of fan #3 (RPM)	
Fan4_speed	04h (Fan)	01h(Threshold Based)		Speed of fan #4 (RPM)	May be absent depending on configuration.
Fan presence	04h (Fan)	7Dh (Kontron instance-specifier)	36	Fan presence	
Fan failure	04h (Fan)	7Dh (Kontron instance-specifier)	37	Indicates a defective fan	
Fan tray pres	04h (Fan)	08h ('digital' Discrete - Present/Absent)	38	Indicates a fan tray presence.	
Temp PCIe	01h(Temperature)	01h(Threshold Based)	40	Customer reported temperature of the PCIe card	Updated by the customer. Refer to <a href="#">Managing customer added sensors</a> .
Temp Heater	01h(Temperature)	01h(Threshold Based)	39	Heater element temperature	
Temp M.2	01h(Temperature)	01h(Threshold Based)	41	Customer reported temperature of M.2	Updated by the customer. Refer to <a href="#">Managing customer added sensors</a> .
Temp SFP1	01h(Temperature)	01h(Threshold Based)	42	Customer reported temperature of SFP1	
Temp SFP2	01h(Temperature)	01h(Threshold Based)	43	Customer reported temperature of SFP2	
IPMI Watchdog	23h (Watchdog 2)	6Fh (Sensor Specific)	44	IPMI Watchdog sensor	

# Interpreting sensor data

{This article describes how to interpret sensor data.}

Table of contents

- [Interpretation procedure](#)
  - [Interpreting non-discrete sensor data](#)
  - [Interpreting discrete sensor data](#)
  - [Accessing event data byte 2 and 3 \(optional\)](#)
- [Interpretation information](#)
  - [Sensor type](#)
  - [Sensor event/reading type](#)
  - [Event data bytes 2 and 3](#)

## Interpretation procedure

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

- Event ID
- Associated sensor
- Description

Refer for [System event log](#) for instructions.

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

Step_1	<p>In ipmitool , the <b>sensor</b> command returns a table. The columns are defined as:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Numerical reading</li> <li>• Event/reading type/unit</li> <li>• Reading bytes 3 and 4</li> <li>• Lower non-recoverable threshold value</li> <li>• Lower critical threshold value</li> <li>• Lower noncritical threshold value</li> <li>• Upper noncritical threshold value</li> <li>• Upper critical threshold value</li> <li>• Upper non-recoverable threshold value</li> </ul>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor CPU            45,000   discrete     0x0000   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status     0x0     discrete     0x0080   na       na       na       na       na       na Temp DIMM A    45,000   degrees C   ok       0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B    52,000   degrees C   ok       0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet     45,000   degrees C   ok       0,000   -41,000   0,000   74,000   84,000   99,000 Temp BMC      58,000   degrees C   ok       0,000   -41,000   0,000   74,000   84,000   124,000 Temp Vcore     68,000   degrees C   ok       0,000   -41,000   0,000   94,000   104,000   124,000 Temp Cortina   57,000   degrees C   ok       0,000   -5,000    0,000   69,000   79,000   124,000</pre>
Step_2	<p>Refer to the third column of the table or the platform <a href="#">Sensor list</a> to verify if the specific sensor is discrete or non-discrete.</p> <p>The third column writes <b>discrete</b> for discrete sensors or a unit type for non-discrete sensors.</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor CPU            45,000   discrete     0x0000   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status     0x0     discrete     0x0080   na       na       na       na       na       na Temp DIMM A    45,000   degrees C   ok       0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B    52,000   degrees C   ok       0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet     45,000   degrees C   ok       0,000   -41,000   0,000   74,000   84,000   99,000 Temp BMC      58,000   degrees C   ok       0,000   -41,000   0,000   74,000   84,000   124,000 Temp Vcore     68,000   degrees C   ok       0,000   -41,000   0,000   94,000   104,000   124,000 Temp Cortina   57,000   degrees C   ok       0,000   -5,000    0,000   69,000   79,000   124,000</pre>
Step_3	<p>Refer to <a href="#">Interpreting non-discrete sensor data</a> or <a href="#">Interpreting discrete sensor data</a> depending on the sensor's event/reading type.</p>	

## Interpreting non-discrete sensor data

## PRELIMINARY

<p><b>Step_1</b></p> <p>If the sensor event/reading type is non-discrete, the numerical reading value is shown in the second column.</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor Temp CPU   85,000   degrees C   nc   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status   0x00   discrete   nc   0x0000   na   na   na   na   na Temp DIMM A   45,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B   52,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet   37,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp BMC   58,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp Vcore   68,000   degrees C   ok   0,000   -41,000   0,000   94,000   104,000   124,000 Temp Curtina   57,000   degrees C   ok   0,000   -5,000   0,000   69,000   79,000   124,000</pre>
<p><b>Step_2</b></p> <p>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.</p> <p>Refer to <a href="#">Threshold based event/reading type</a> for the definitions of threshold states.</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor Temp CPU   85,000   degrees C   nc   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status   0x00   discrete   nc   0x0000   na   na   na   na   na Temp DIMM A   45,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B   52,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet   37,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp BMC   58,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp Vcore   68,000   degrees C   ok   0,000   -41,000   0,000   94,000   104,000   124,000 Temp Curtina   57,000   degrees C   ok   0,000   -5,000   0,000   69,000   79,000   124,000</pre>
<p><b>Step_3</b></p> <p>An event will be created according to the assertion enabled for the specified sensor.</p> <p>RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sensor get [Sensor_ID]</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor get "Temp CPU" Locating sensor record... Sensor ID : Temp CPU (0x5) Entity ID : 7,0 Sensor Type (Threshold) : Temperature Sensor Reading : 55 (+/- 1) degrees C Status : ok Lower Non-Recoverable : 0,000 Lower Critical : -1,000 Lower Non-Critical : 0,000 Upper Non-Critical : 84,000 Upper Critical : 99,000 Upper Non-Recoverable : 124,000 Positive Hysteresis : 4,000 Negative Hysteresis : 4,000 Assertion_Events :  Assertions Enabled : lcr- ucr+ unr+ Deassertions Enabled : lcr- ucr+ unr+</pre>

## Interpreting discrete sensor data

<p><b>Step_1</b></p> <p>The second column of the <b>sensor</b> command should be ignored if the sensor is of discrete type. By default, discrete sensors should have a numerical reading value of <b>0x0</b>.</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor Temp CPU   85,000   degrees C   nc   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status   0x0   discrete   nc   0x0080   na   na   na   na   na Temp DIMM A   45,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B   52,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet   37,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp BMC   58,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp Vcore   68,000   degrees C   ok   0,000   -41,000   0,000   94,000   104,000   124,000 Temp Curtina   57,000   degrees C   ok   0,000   -5,000   0,000   69,000   79,000   124,000</pre>
<p><b>Step_2</b></p> <p>The fourth column of the table is an aggregation of bytes 3 and 4 of the response given on sensor reading. Byte 3 is the less significant byte in the aggregation of bytes 3 and 4.</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor Temp CPU   85,000   degrees C   nc   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status   0x0   discrete   nc   0x0080   na   na   na   na   na Temp DIMM A   45,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B   52,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet   37,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp BMC   58,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp Vcore   68,000   degrees C   ok   0,000   -41,000   0,000   94,000   104,000   124,000 Temp Curtina   57,000   degrees C   ok   0,000   -5,000   0,000   69,000   79,000   124,000</pre>
<p><b>Step_3</b></p> <p>As for byte 3, all values should be <b>0x80</b>, meaning all event messages are enabled for this sensor.</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor Temp CPU   85,000   degrees C   nc   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status   0x0   discrete   nc   0x0080   na   na   na   na   na Temp DIMM A   45,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B   52,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet   37,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp BMC   58,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp Vcore   68,000   degrees C   ok   0,000   -41,000   0,000   94,000   104,000   124,000 Temp Curtina   57,000   degrees C   ok   0,000   -5,000   0,000   69,000   79,000   124,000</pre>
<p><b>Step_4</b></p> <p>As for byte 4, it represents the states/event offsets defined for each type in the IPMI specification. Refer to <a href="#">Sensor event/reading type</a> for lists of possible states for each sensor.</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor Temp CPU   85,000   degrees C   nc   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status   0x0   discrete   nc   0x0080   na   na   na   na   na Temp DIMM A   45,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B   52,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet   37,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp BMC   58,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp Vcore   68,000   degrees C   ok   0,000   -41,000   0,000   94,000   104,000   124,000 Temp Curtina   57,000   degrees C   ok   0,000   -5,000   0,000   69,000   79,000   124,000</pre>
<p><b>Step_5</b></p> <p>If specified in the event/reading type description of the sensor, refer to <a href="#">Event data bytes 2 and 3</a> for additional information.</p>	<pre>\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor Temp CPU   85,000   degrees C   nc   0,000   -1,000   0,000   84,000   99,000   124,000 CPU Status   0x0   discrete   nc   0x0080   na   na   na   na   na Temp DIMM A   45,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp DIMM B   52,000   degrees C   ok   0,000   -41,000   0,000   74,000   84,000   99,000 Temp Inlet   37,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp BMC   58,000   degrees C   ok   0,000   -41,000   0,000   54,000   66,000   70,000 Temp Vcore   68,000   degrees C   ok   0,000   -41,000   0,000   94,000   104,000   124,000 Temp Curtina   57,000   degrees C   ok   0,000   -5,000   0,000   69,000   79,000   124,000</pre>

## Accessing event data byte 2 and 3 (optional)

**NOTE:** This part of the procedure is needed only if the sensor concerned specifies it. Refer to [Sensor event/reading type](#). Event data can be obtained:

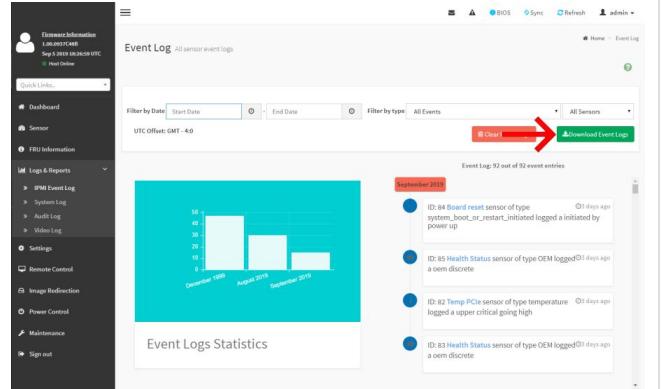
- Using the [BMC Web UI](#)
- Using [IPMI](#)

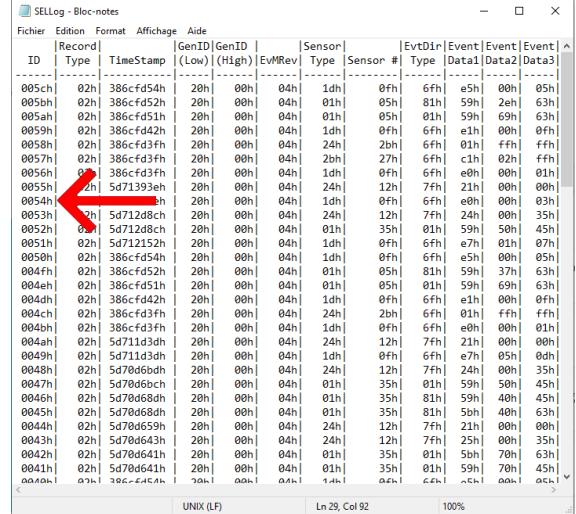
## Accessing event data bytes 2 and 3 using the Web UI

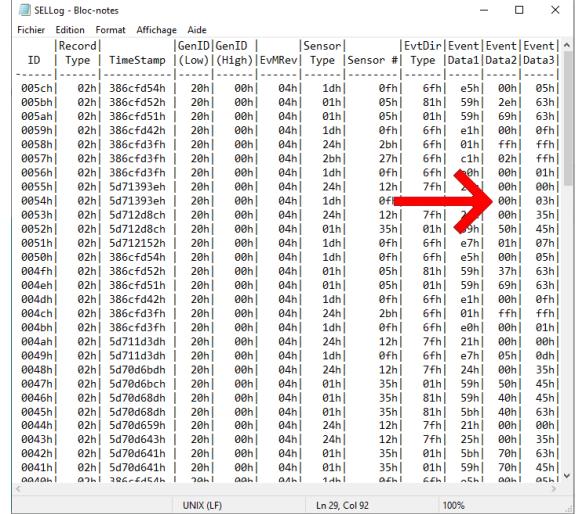
Refer to [Accessing a BMC using the Web UI](#) for access instructions.

# PRELIMINARY

Step_1	Convert the event ID to hexadecimal.
Step_2	Access the BMC Web UI of the server.
Step_3	Download the system event logs and open the file with any text editor.
Step_4	In the SELLog file, find the event using its ID.
Step_5	Event Data 2 and 3 can be found in the last two columns. Refer to <a href="#">Event data bytes 2 and 3</a> to interpret the event data bytes.







## Accessing event data bytes 2 and 3 using IPMI

The following procedures will be executed using the [Accessing a BMC using IPMI over LAN \(IOL\)](#) method, but some tasks can also be performed using KCS ([Accessing a BMC on an ME module using IPMI \(KCS\)](#)). To use KCS, remove the IOL parameters from the command: `-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password]`.

## PRELIMINARY

Step_1	Convert the event ID to hexadecimal.	
Step_2	<p>Print the event's detailed information using the hexadecimal conversion of the ID.</p> <pre>RemoteServer_OSPrompt:~\$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sel get [Event_ID]</pre>	<pre>\$ ipmitool -I lanplus -H 172.16.206.10 -U admin -P admin sel get 0x51 SEL Record ID      : 0051 Record Type        : 02 Timestamp          : 2019-09-05 2019-09-05 Generator ID       : 0020 EvM Revision       : 04 Sensor Type        : System Boot Initiated Sensor Number      : 0F Event Type         : Sensor-specific Discrete Event Direction    : Assertion Event Event Data (RAW)   : e70107 Event Interpretation: Missing Description         : System Restart  Sensor ID          : Board reset (0xf) Entity ID          : 7.96 Sensor Type (Discrete): System Boot Initiated States Asserted    : System Boot Initiated [System Restart]</pre>
Step_3	<p>Recover the event data bytes and the <b>Sensor Number</b>.</p> <p>The <b>Event Data (RAW)</b> row is an aggregation of the three event data bytes, where the first byte is the most significant byte and the third one is the less significant one.</p> <p><b>NOTE:</b> The first data byte should always be ignored.</p>	<pre>\$ ipmitool -I lanplus -H 172.16.206.10 -U admin -P admin sel get 0x51 SEL Record ID      : 0051 Record Type        : 02 Timestamp          : 2019-09-05 2019-09-05 Generator ID       : 0020 EvM Revision       : 04 Sensor Type        : System Boot Initiated Sensor Number      : 0F Event Type         : Sensor-specific Discrete Event Direction    : Assertion Event Event Data (RAW)   : <b>e70107</b> Event Interpretation: Missing Description         : System Restart  Sensor ID          : Board reset (0xf) Entity ID          : 7.96 Sensor Type (Discrete): System Boot Initiated States Asserted    : System Boot Initiated [System Restart]</pre>
Step_4	Refer to <a href="#">Event data bytes 2 and 3</a> to interpret the event data bytes.	

## Interpretation information

Each sensor has a [Sensor type attribute](#) and a [Sensor event/reading type](#) attribute. When a sensor created an event specified, more data about the event can be found in [Event data bytes 2 and 3](#). For more information about IPMI sensors refer to the IPMI documentation.

For a list of all the platform sensors, refer to [Sensor list](#).

### Sensor type

The sensor type attribute defines what the sensor is monitoring.

The following table lists all the IPMI sensor types present on the platform.

# PRELIMINARY

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.
04h (Fan)	General information about the fan(s) of the platform (e.g. speed, presence, failure).
07h (Processor)	General information about the processor (e.g. presence, failure, health status).
08h (Power supply)	General information about the power supply (e.g. presence, failure, health status).
10h (Event logging disable)	General information about the platform system event log.
1Dh (System boot/restart initiated)	Report the last restart/reboot source.
23h (Watchdog)	General information about the IPMI watchdog.
24h (Platform alert)	Report information about alerts generated by the BMC.
25h (Presence)	Report an entity presence on the platform.
2Bh (Version change)	Report the state of hardware, firmware or software version.
D3h (OEM jumper status)	Kontron custom jumper status sensor type. Refer to <a href="#">OEM event/reading type</a> .

## Sensor event/reading type

The sensor event/reading type attribute defines how the reading of the value should be interpreted and how the sensor-related events are triggered. All event/reading types can either be discrete or non-discrete.

The following table describes the different event/reading types present on the platform.

Event/reading type	7-bit event type code	Description	Offset
Threshold based	01h	Non-discrete, meaning it has a numerical reading and event triggers.	Offsets are standard and defined in the <a href="#">Threshold-based event/reading type</a> table.
Sensor-specific	6Fh	Discrete, meaning it has no numerical values, but it has event triggers.	Offsets are specific to the sensor's type and defined in the <a href="#">Sensor-specific event/reading type</a> table.
OEM	70h-7Fh	Discrete and defined by the OEM	Offsets are OEM specific and defined in the <a href="#">OEM event/reading type</a> table.

## Threshold based event/reading type

This type of sensor creates events as the numerical reading of a sensor reaches a pre-established threshold value. Threshold-based sensors on this platform can either report a voltage, a temperature or a fan speed.

## PRELIMINARY

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

### Sensor-specific event/reading type

A sensor-specific event/reading type is a discrete type of sensor, meaning that it has no numerical value. When a sensor is of type sensor-specific, the event offset values are defined by the sensor type.

**NOTE:** Not all sensor-specific event offsets are supported by the platform. The following table lists the sensor-specific event offsets implemented on the platform.

## PRELIMINARY

ID	Sensor name	Sensor type	Specific offset	Event trigger/state
2	CPU Status	07h (Processor)	00h	IERR
			01h	Thermal trip
			05h	Configuration error
9	Board Reset	1Dh (System boot restart initiated)	00h	Initiated by power up
			01h	Initiated by hard reset
			05h	OS / run-time software initiated hard reset
			07h	System restart
10	PWROK Capture1	08h (Power supply)	00h	Power supply presence detected
11	PWROK Capture 2		01h	Power supply failure detected
26	Ver Change FPGA  NOTE: See event data table below for more information.	2Bh (Version change)	00h	Hardware change detected with associated entity - success or failure not implied
			01h	Firmware or software change detected with associated entity - success or failure not implied
			02h	Hardware incompatibility detected with entity
27	Ver Change BIOS  NOTE: See event data table below for more information.		03h	Firmware or software incompatibility detected with entity
			04h	Entity is of an invalid or unsupported firmware or software version
			05h	Entity contains an invalid or unsupported firmware or software version
			06h	Hardware change detected with associated entity was successful
28	Ver Change BMC  NOTE: See event data table below for more information.		07h	Firmware or software change detected with associated entity was successful
31	Jumper Status	D3h (OEM jumper status)	Refer to <a href="#">OEM event/reading type</a> .	
32	BMC SEL State	10h (Event logging disable)	02h	System event log cleared
			04h	System event log full
			05h	System event log almost full
45	IPMI Watchdog  NOTE: See event data table below for more information.	23h (Watchdog 2)	00h	Timer expired
			01h	Hard reset
			02h	Power down
			03h	Power cycle
			08h	Timer interrupt

### OEM event/reading type

## PRELIMINARY

An OEM event/reading type is a discrete type of sensor, meaning that it has no numerical value. When a sensor is of type OEM, the event offset values are defined in the following table.

ID	Sensor name	Reading type code	Event type code	Specific offset	Event trigger/state
25	Health status <b>NOTE:</b> See event data table below for more information.	24h (Platform alert)	7Fh (OEM health severity status sensor)	00h	Status not available in current state
				01h	Healthy
				02h	Informational fault
				03h	Minor fault
				04h	Major fault
				05h	Critical fault
31	Jumper Status	D3h (OEM jumper status)	6Fh (Sensor specific)	00h	Jumper present on pins 1–2 (IPMI override)
				01h	Jumper present on pins 3–4 (BMC - not used)
				02h	Jumper present on pins 5–6 (watchdog disabled)
				03h	Jumper present on pins 7–8 (fan override)
				04h	Jumper present on pins 9–10 (FPGA - spare jumper 1)
				05h	Jumper present on pins 11–12 (CPU clear bios setup in FLASH)
				06h	Jumper present on pins 13–14 (FPGA - spare jumper 2)
37	Fan presence	04h (Fan)	7Dh (Kontron instance specifier)	00h	Fan1
				01h	Fan2
38	Fan failure			02h	Fan3
				03h	Fan4
39	Fan tray pres	04h (Fan)	08h ("Digital" discrete)	00h	Fan tray missing (device absent)
				01h	Fan tray inserted (device present)

### Event data bytes 2 and 3

When a sensor triggers an event in the system event log, event data bytes 2 and 3 might contain additional information about the event.

These event data bytes must be read solely on the specific offset listed in the following tables.

**NOTE:** Event data byte values are not event offsets. They are hexadecimal values and should be interpreted differently than event offsets.

### Generic event data byte description

This table defines the event data bytes 2 and 3 for generic IPMI sensors.

ID	Sensor	Specific offset	Event data 2	Event data 3
9	Board reset	• 07h	[7:4] - Reserved bits [3:0] - Restart cause given by the raw IPMI <i>Get System Restart</i> command: • 0x00 = Unknown start/restart cause • 0x01 = Chassis control command	Report the channel number from which the command was received.

## PRELIMINARY

CRS: Chassis Control Subcommand

- 0x02 = Reset via push button
- 0x04 = Watchdog expiration
- 0x05 = OEM
- 0x06 = Automatic power-up on AC being applied due to "always restore" power restore policy
- 0x07 = Automatic power-up on AC being applied due to "restore previous power state" power restore policy
- 0x08 = Reset via PEF
- 0x09 = Power cycle via PEF
- 0x0A = Soft reset
- 0x0B = Power up via RTC
- All other are reserved or unsupported

26	Ver Change FPGA	<ul style="list-style-type: none"> <li>• 00h</li> <li>• 01h</li> <li>• 02h</li> <li>• 03h</li> <li>• 04h</li> <li>• 05h</li> <li>• 06h</li> <li>• 07h</li> </ul>	<p>Reports additional events about the version change:</p> <ul style="list-style-type: none"> <li>• 0x00 = Unspecified</li> <li>• 0x01 = BMC ID change</li> <li>• 0x02 = BMC firmware revision</li> <li>• 0x03 = BMC device revision</li> <li>• 0x04 = BMC manufacturer ID</li> </ul>	Not used for this sensor.
27	Ver Change BIOS			
28	Ver Change BMC		<ul style="list-style-type: none"> <li>• 0x05 = BMC IPMI version</li> <li>• 0x06 = BMC auxiliary firmware ID</li> <li>• 0x07 = BMC firmware boot block</li> <li>• 0x08 = Other BMC firmware</li> <li>• 0x09 = BIOS/UEFI change</li> <li>• 0x0A = SMBIOS change</li> <li>• 0x0B = OS change</li> <li>• 0x0C = OS loader change</li> <li>• 0x0D = Service or diagnostic partition change</li> <li>• 0x0E = Management software agent change</li> <li>• 0x0F = Management software application change</li> <li>• 0x10 = Management software middleware change</li> <li>• 0x11 = Programmable hardware change</li> <li>• 0x12 = FRU module change</li> <li>• 0x13 = FRU component ca</li> <li>• 0x14 = FRU replaced with equivalent version</li> <li>• 0x15 = FRU replaced with newer version</li> <li>• 0x16 = FRU replaced with older version</li> <li>• 0x17 = FRU hardware configuration change</li> </ul>	
45	IPMI Watchdog	<ul style="list-style-type: none"> <li>• 00h</li> <li>• 01h</li> <li>• 02h</li> <li>• 03h</li> <li>• 08h</li> </ul>	<p>[7:4] - Interrupt type:</p> <ul style="list-style-type: none"> <li>• 0x00 = None</li> <li>• 0x10 = SMI</li> <li>• 0x20 = NMI</li> <li>• 0x30 = Messaging interrupt</li> <li>• 0xF0 = Unspecified</li> </ul> <p>[3:0] - Timer use at expiration:</p> <ul style="list-style-type: none"> <li>• 0x00 = Reserved</li> <li>• 0x01 = BIOS/FRB2</li> <li>• 0x02 = BIOS/POST</li> <li>• 0x03 = OS load</li> <li>• 0x04 = SMS/OS</li> <li>• 0x05 = OEM</li> <li>• 0x0F = Unspecified</li> </ul>	Not used for this sensor.

## PRELIMINARY

### OEM event data byte description

This table defines the event data bytes 2 and 3 for OEM-defined sensors.

ID	Sensor	Specific offset	Event data 2	Event data 3
25	Health status	<ul style="list-style-type: none"><li>• 02h</li><li>• 03h</li><li>• 04h</li><li>• 05h</li></ul>	Report the ID of the sensor that caused the health status event.	Not used for this sensor.

## Managing customer added sensors

*{This article provides informations and instructions to monitor and integrate customer-specific sensors in the cooling mechanism of the platform}*

### Table of contents

- [Address offset](#)
- [Temperature format](#)
- [Script example](#)

To implement a new sensor in your system, this sensor needs to be read by the platform server and the value must be sent to the BMC to be used for fan management. Your custom software must periodically writes this data, otherwise there will be no value provided to the BMC. If the data is not written within a 5-second time period, it will be published as n/a.

The sensors that need to be updated by the user are:

- Temp PCIe
- Temp SFP1
- Temp SFP2
- Temp M.2

**NOTE:** User sensor names are arbitrary as they are registers. These names cannot be changed by the end user.

<b>NOTICE</b>	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.
---------------	--

## Address offset

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

Sensor	Address offset
Temp PCIe	2600
Temp M.2	2601
Temp SFP1	2602
Temp SFP2	2603

## Temperature format

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

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

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

- -1°C is the smallest negative value available and corresponds to 0xFF.
- -127°C is the largest negative value and corresponds to 0x81.

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

## Script example

The following example is a Shell Script (.sh) file executed in the operating system. It updates the value of the Temp PCIe sensor to 37°C (0x25 in hexadecimal) every second.

## PRELIMINARY

Update Temp PCIe

```
#!/bin/bash
while true
do
    sleep 1 #NOTE Value is written every sec, this avoid being cleared if not refresh in the last 5 seconds
    printf "\x25" | dd seek=2600 bs=1 count=1 of=/dev/port 2> /dev/null
done
```

NOTE: This script is executed in CentOS 7.4 and should be adapted for other operating systems.

## Maintenance

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

Children

- [System event log](#)
- [Component replacement](#)
- [\[Content under creation\] Backup and restore](#)
- [Upgrading](#)
- [\[Content under creation\] Scaling](#)

## System event log

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

Table of contents

- [Using the BMC Web UI](#)
  - [Accessing the system event log](#)
  - [Clearing the system event log](#)
  - [Downloading the system event log](#)
- [Using IPMI via KCS](#)
  - [Accessing the system event log](#)
  - [Clearing the system event log](#)
- [Using Redfish](#)
  - [Accessing the system event log](#)
  - [Clearing the system event log](#)

The system event log can be accessed:

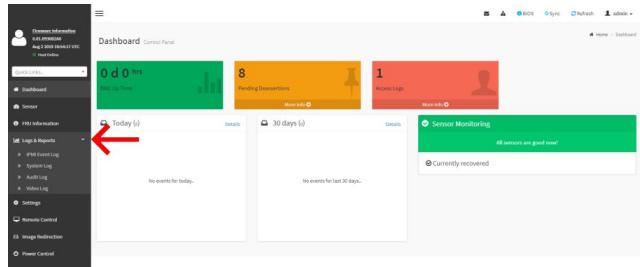
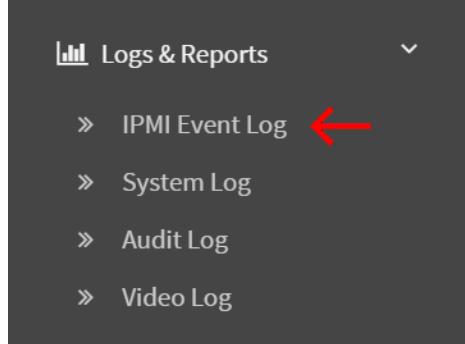
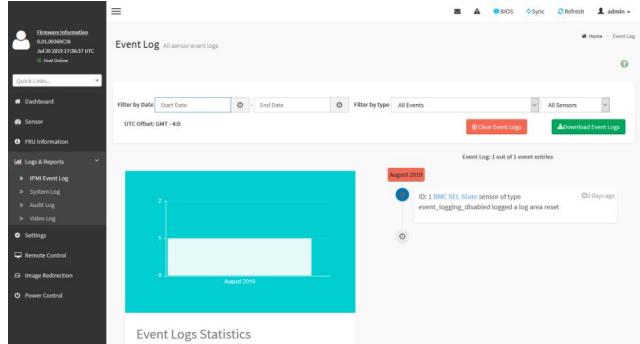
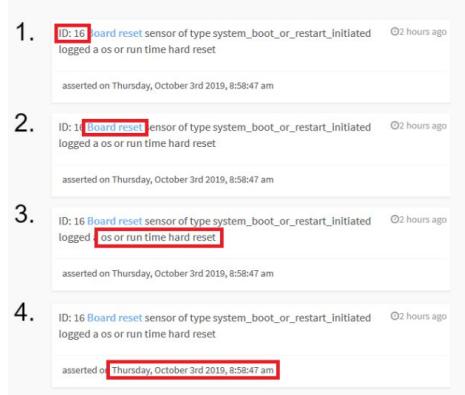
- Using the [BMC Web UI](#)
- Using [IPMI](#)
- Using [Redfish](#)

## Using the BMC Web UI

### Accessing the system event log

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

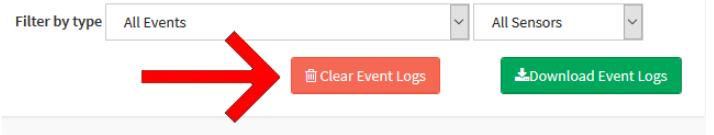
# PRELIMINARY

Step_1	Access the BMC Web UI of the server.	
Step_2	Select <b>Logs &amp; Reports</b> from the left side menu.	
Step_3	Select <b>IPMI Event Log</b> from the dropdown menu.	
Step_4	The system event log is displayed.	
Step_5	Click on an event and collect the following information: 1. Event ID 2. Associated sensor 3. Description 4. Time asserted	 <p>1. ID: 16 Board reset sensor of type system_boot_or_restart_initiated asserted on Thursday, October 3rd 2019, 8:58:47 am</p> <p>2. ID: 16 Board reset sensor of type system_boot_or_restart_initiated asserted on Thursday, October 3rd 2019, 8:58:47 am</p> <p>3. ID: 16 Board reset sensor of type system_boot_or_restart_initiated asserted on Thursday, October 3rd 2019, 8:58:47 am</p> <p>4. ID: 16 Board reset sensor of type system_boot_or_restart_initiated asserted on Thursday, October 3rd 2019, 8:58:47 am</p>

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

## Clearing the system event log

## PRELIMINARY

Step_1	<p>In the Event Log menu, select <b>Clear Event Logs</b>.</p>	
Step_2	<p>Confirm the action by clicking on <b>OK</b>.</p>	<p>You are about to clear the IPMI Event Log. Do you really want to clear the IPMI Event Log?</p> <p><input type="checkbox"/> Empêcher cette page d'ouvrir des dialogues supplémentaires</p> <div style="text-align: right; margin-top: 10px;"> <span style="border: 1px solid blue; padding: 2px 10px; border-radius: 5px; cursor: pointer;">OK</span> <span style="margin-left: 10px;">Annuler</span> </div>

### Downloading the system event log

Step_1	<p>In the Event Log menu, select <b>Download Event Logs</b>.</p>	
--------	--	--

## Using IPMI via KCS

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

### Accessing the system event log

Step_1	<p>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, access the system event log information.</p> <p>LocalServer_OSPrompt:~\$ ipmitool sel</p>	<pre>\$ ipmitool sel SEL Information Version      : 1.5 (v1.5, v2 compliant) Entries     : 52 Free Space   : 64566 bytes Percent Used : 1% Last Add Time : 1999-12-31 14:00:17 EST Last Del Time : Not Available Overflow     : false Supported Cmds : 'Delete' 'Partial Add' 'Reserve' 'Get Alloc Info' # of Alloc Units : 3639 Alloc Unit Size : 18 # Free Units   : 3587 Largest Free Blk : 3587 Max Record Size : 1</pre>
Step_2	<p>Access the system event log list.</p> <p>LocalServer_OSPrompt:~\$ ipmitool sel elist</p>	<pre>\$ ipmitool sel elist 1   2019-09-12   06:07:21 EDT   Event Logging Disabled BMC SEL State   Log area reset/cleared 2   2019-09-12   06:13:45 EDT   Temperature Temp CPU   Upper Critical going high   Asserted     Reading 32 &gt; Threshold 99 degrees C 3   2019-09-12   06:13:46 EDT   Platform Alert Health Status     Asserted 4   2019-09-12   06:14:24 EDT   Temperature Temp CPU   Upper Critical going high   Deasserted   Reading 32 &gt; Threshold 99 degrees C 5   2019-09-12   06:14:25 EDT   Platform Alert Health Status     Asserted 6   2019-09-12   06:26:45 EDT   Temperature Temp PCIE   Upper Critical going high   Asserted     Reading 80 &gt; Threshold 69 degrees C 7   2019-09-12   06:26:48 EDT   Platform Alert Health Status     Asserted 8   2019-09-12   06:31:44 EDT   Platform Alert Health Status     Asserted 9   2019-09-12   06:31:49 EDT   Platform Alert Health Status     Asserted a   2019-09-12   06:34:30 EDT   Platform Alert Health Status     Asserted b   2019-09-12   06:34:43 EDT   Platform Alert Health Status     Asserted</pre>
Step_3	<p>Collect the following information for the specified event:</p> <ul style="list-style-type: none"> <li>• Event ID - 1st column</li> <li>• Time asserted - 2nd and 3rd column</li> <li>• Associated sensor - 4th column (optional)</li> <li>• Description - 5th column</li> </ul>	

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

## Clearing the system event log

Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, clear the system event log. LocalServer_OSPrompt:~# ipmitool sel clear	<pre>\$ ipmitool sel clear Clearing SEL. Please allow a few seconds to erase.</pre>
Step_2	Verify that the system event log was properly cleared. LocalServer_OSPrompt:~# ipmitool sel elist	<pre>\$ ipmitool sel elist 1   2019-08-15   10:16:48 EDT   Event Logging Disabled BMC SEL State   Log area reset/cleared   Asserted</pre>

## Using Redfish

### Accessing the system event log

Refer to [Accessing a BMC using Redfish](#) for access instructions.

Step_1	From a remote computer that has access to the management network subnet, open a command prompt and access the system event log. RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]Managers/Self/LogServices/SEL/Entries   jq	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.243/redfish/v1/Managers/Self/LogServices/SEL/Entries   jq {   "@odata.context": "/redfish/v1/Managers/Self/LogServices/SEL/Entries/\$metadata\$LogEntryCollection",   "@odata.etag": "W/\"1590027789\"",   "@odata.id": "/redfish/v1/Managers/Self/LogServices/SEL/Entries",   "@odata.type": "#LogEntry.v1_3_0.LogEntry",   "Description": "Collection of entries for this log service",   "Members": [     {       "@odata.id": "/redfish/v1/Managers/Self/LogServices/SEL/Entries/1",       "@odata.type": "#LogEntry.v1_3_0.LogEntry",       "Created": "2019-09-30T19:00:00-05:00",       "Description": "Asset asserted",       "EntryCode": "Asset",       "EventTimestamp": "1999-12-31T19:00:13-05:00",       "Id": "1",       "Links": {         "OriginOfCondition": {           "@odata.id": "/redfish/v1/"         }       },       "Message": "",       "MessageArgs": [],       "MessageId": "OK",       "Name": "SEL 1",       "SensorNumber": 0,       "Severity": "OK"     }   ],   "MembersCount": 1,   "MembersTotal": 1 }</pre>
Step_2	Collect the following information for the specified event: <ul style="list-style-type: none"><li>• Description or the <b>EntryCode</b> attribute</li><li>• Time asserted or the <b>EventTimestamp</b> attribute</li><li>• Event ID or the <b>Id</b> attribute</li><li>• Associated sensor or the <b>SensorNumber</b> attribute (optional)</li></ul>	<pre>{   "Members": [     {       "@odata.id": "/redfish/v1/Managers/Self/LogServices/SEL/Entries/1",       "@odata.type": "#LogEntry.v1_3_0.LogEntry",       "Created": "2019-09-30T19:00:00-05:00",       "Description": "...",       "EntryCode": "Asset",       "EventTimestamp": "1999-12-31T19:00:16-05:00",       "Id": "1",       "Links": {         "OriginOfCondition": {           "@odata.id": "/redfish/v1/"         }       },       "Message": "...",       "MessageArgs": [],       "MessageId": "OK",       "Name": "SEL 1",       "SensorNumber": 43,       "Severity": "Platform Alert"     }   ] }</pre>

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

### Clearing the system event log

## PRELIMINARY

Step_1	<p>From a remote computer that has access to the management network subnet, open a command prompt and clear the system event log.</p> <pre>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]Managers/Self/LogServices/SEL/Actions/LogService.ClearLog -X POST -d'{"ClearType":"ClearAll"}' -H "Content-Type: application/json"   jq</pre> <div style="background-color: black; color: white; padding: 5px;"><pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Managers/Self/LogServices/SEL/Actions/LogService.ClearLog -X POST -d'{"ClearType":"ClearAll"}' -H "Content-Type: application/json"   jq</pre></div>
Step_2	<p>Verify that the system event log was properly cleared.</p> <pre>RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]Managers/Self/LogServices/SEL/Entries   jq</pre> <div style="background-color: black; color: white; padding: 5px;"><pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Managers/Self/LogServices/SEL/Entries   jq {   "@odata.context": "/redfish/v1/\$metadata#LogEntryCollection.LogEntryCollection",   "@odata.id": "/redfish/v1/Managers/Self/LogServices/SEL/Entries",   "@odata.type": "#LogEntryCollection.LogEntryCollection",   "Description": "Collection of entries for this log service",   "Members": [],   "Members@odata.count": 0,   "Name": "Log Service Entries Collection" }</pre></div>

## Component replacement

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

---

The only built-in component of the ME1100 platform that can be replaced is the fan tray assembly.  
Refer to [Component installation and assembly](#) for the replacement procedure.

# Upgrading

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

Table of contents

- [Upgrading the firmware of the BMC, BIOS and FPGA using ipmitool](#)
  - [Prerequisites](#)
  - [Procedure](#)
    - [From BMC version 2.xx to >2.xx](#)
    - [From BMC version 1.xx to >2.xx](#)
- [Upgrading the firmware of the BMC using the Web UI](#)

## Upgrading the firmware of the BMC, BIOS and FPGA using ipmitool

### Prerequisites

1	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2	The remote computer has access to the management network subnet.
3	A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.
4	The latest HPM package has been downloaded.

#### Relevant section:

[Baseboard management controller - BMC](#)



All BIOS settings, including the boot order and CSM support, are reset to their default value after a BIOS upgrade.

This may include breaking secure boot chain which will render your OS unbootable.

### Procedure

#### From BMC version 2.xx to >2.xx

Step_1	<p>From a remote computer that has access to the management network subnet, enter the desired command.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power off</pre> <p><b>NOTE:</b> The upgrade can be done without a power off and the power status verification; however, when an all activate command is executed, a complete system reboot will occur.</p>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power off Chassis Power Control: Down/Off</pre>
Step_2	<p>Confirm the server power status is OFF.</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP]</pre>	<pre>\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status Chassis Power is off</pre>

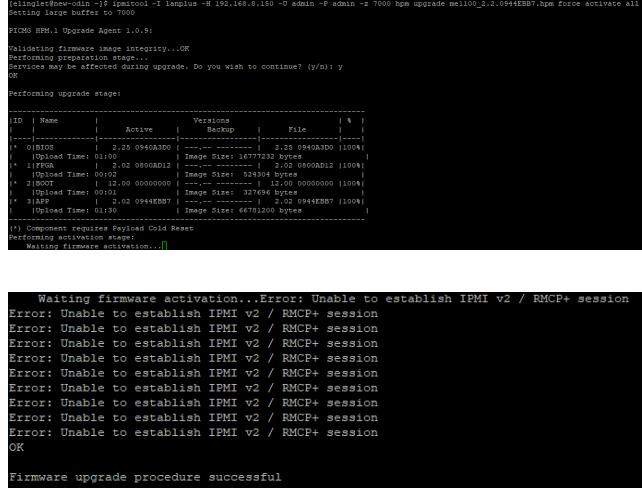
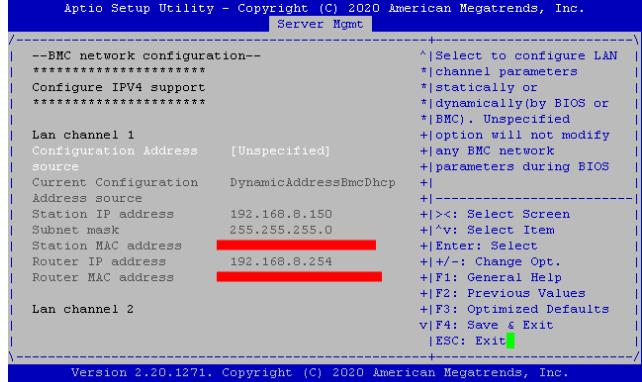
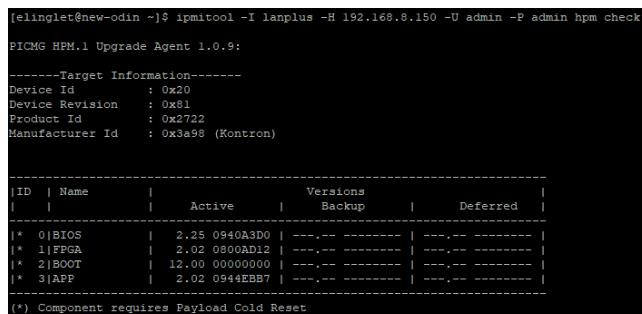
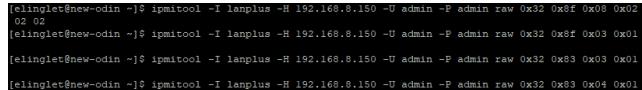
## PRELIMINARY

	<pre>I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power status</pre>	
Step_3	<p>Verify that the upgrade version is adequate.</p> <pre>I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] hpm check &lt;HPM bundle(HPM file)&gt;</pre>	<pre>\$ ipmitool -I lanplus -H 172.16.205.245 -U admin -P admin hpm check me110x_0.1.09369C38.hpm PICMG HPM.1 Upgrade Agent 1.0.9: Validating firmware image integrity...OK Performing preparation stage...OK Comparing Target &amp; Image File version   ID   Name   Active   Versions   File    --- --- --- --- ---    * 0   BIOS   2.20 093694DD   ---.---   2.14 093694DD     * 1   FPGA   2.02 0800AD12   ---.---   2.02 0800AD12     * 2   BOOT   12.00 00000000   ---.---   12.00 00000000     * 3   APP   0.01 09369C38   ---.---   0.01 09369C38   (*) Component requires Payload Cold Reset (*) Indicates component would be upgraded</pre>
Step_4	<p>Proceed with firmware upgrade.</p> <pre>I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] -z 7000 hpm upgrade &lt;HPM bundle(HPM file) &gt; all activate</pre> <p><b>NOTE:</b> Wait for the upgrade to finish before performing any action on the platform. If the upgrade is interrupted, it might corrupt the data.</p>	<pre>\$ ipmitool -I lanplus -H 172.16.205.245 -U admin -P admin -z 1024 hpm upgrade me110x_0.1 all activate Setting large buffer to 1024 PICMG HPM.1 Upgrade Agent 1.0.9: Validating firmware image integrity...OK Performing preparation stage... Services may be affected during upgrade. Do you wish to continue? (y/n): y OK Performing upgrade stage:   ID   Name   Active   Versions   File   %    --- --- --- --- --- ---    * 0   BIOS   2.20 093694DD   ---.---   2.14 093694DD   100%       Upload Time: 05:32         Image Size: 16777232 bytes     * 1   FPGA   2.02 0800AD12   ---.---   2.02 0800AD12   Skip     * 2   BOOT   12.00 00000000   ---.---   12.00 00000000   Skip     * 3   APP   0.01 09369C38   ---.---   0.01 09369C38   100%       Upload Time: 07:25         Image Size: 66781200 bytes  </pre>
Step_5	<p>Verify that the different components upgraded properly.</p> <pre>I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] hpm check</pre>	<pre>\$ ipmitool -I lanplus -H 172.16.205.245 -U admin -P admin hpm check PICMG HPM.1 Upgrade Agent 1.0.8: -----Target Information----- Device Id : 0x20 Device Revision : 0x1 Product Id : 0x2722 Manufacturer Id : 0x3a98 (Kontron)    ID   Name   Versions         Active   Backup    --- --- --- ---    *0   BIOS   2.20 093694DD   ---.---     *1   FPGA   2.02 0800AD12   ---.---     *2   BOOT   12.00 00000000   ---.---     *3   APP   0.01 09369C38   ---.---   (*) Component requires Payload Cold Reset</pre>

### From BMC version 1.xx to >2.xx

Step_1	<p>From a remote computer that has access to the management network subnet, enter the following command:</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] mc reset cold</pre> <p>And wait 5 minutes to allow all of the BMC's processes to boot up</p>	<pre>[elinglet@new-odin ~]\$ ipmitool -I lanplus -H 192.168.8.150 -U admin -P admin mc reset cold Sent cold reset command to MC [elinglet@new-odin ~]\$</pre>
Step_2	<p>After 5 minutes, issue below commands one by one from a remote computer where ipmi is installed</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin raw 0x32 0x8f 0x03 0x03</pre>	<pre>[elinglet@new-odin ~]\$ ipmitool -I lanplus -H 192.168.8.150 -U admin -P admin raw 0x32 0x8f 0x03 0x03 [elinglet@new-odin ~]\$ ipmitool -I lanplus -H 192.168.8.150 -U admin -P admin raw 0x32 0x8f 0x04 0x03 [elinglet@new-odin ~]\$ ipmitool -I lanplus -H 192.168.8.150 -U admin -P admin raw 0x32 0x83 0x02 0x01 [elinglet@new-odin ~]\$ ipmitool -I lanplus -H 192.168.8.150 -U admin -P admin raw 0x32 0x83 0x00 0x00 [elinglet@new-odin ~]\$ ipmitool -I lanplus -H 192.168.8.150 -U admin -P admin raw 0x32 0x83 0x00 0x00 [elinglet@new-odin ~]\$ ipmitool -I lanplus -H 192.168.8.150 -U admin -P admin raw 0x32 0x83 0x00 0x00 [elinglet@new-odin ~]\$ ipmitool -I lanplus -H 192.168.8.150 -U admin -P admin raw 0x32 0x83 0x00 0x00 [elinglet@new-odin ~]\$</pre>

# PRELIMINARY

	<pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin raw 0x32 0x8f 0x04 RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin raw 0x32 0x83 0x02 0x01 RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin raw 0x32 0x83 0x00 0x00 RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin raw 0x32 0x83 0x03 0x00 RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin raw 0x32 0x83 0x04 0x00</pre>	
Step_3	<p>From a remote computer which has access to the upgrade hpm file, send the following upgrade command:</p> <pre>RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin -z 7000 hpm upgrade &lt;file path&gt; force activate all</pre> <p><b>Note 1:</b> It takes 10 to 20 minutes for the upgrade to complete;</p> <p><b>Note 2:</b> Sometimes you may not get a "Firmware Successful" message, instead you will get timeout error and "Firmware Upgrade Failed". This is because the system lost its IP connectivity after the upgrade and is expected, proceed to next step.</p>	
Step_4	<p>After the update is complete, BMC network parameters will be reset. Reboot the payload, then press F2 to get into the BIOS. Once in the BIOS menu, go to Server Mgmt -&gt; BMC Network configuration menu to configure BMC IP address. After the configuration is done, exit the BIOS by selecting save changes and reset. Note: Network interfaces are now swapped. Lan channel 1 is the RJ45 port and Lan channel 2 is the leftmost SFP port. Configure according to your topology</p>	
Step_5	<p>After you can ping the newly configured BMC, WAIT FOR 5 MINUTES and then send the following command to confirm that the upgrade has been applied properly:</p> <pre>ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin hpm check</pre>	
Step_6	<p>Finally, issue the following raw commands:</p> <pre>ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin raw 0x32 0x8f 0x08 0x02 ipmitool -I lanplus -H &lt;bmc_ip&gt; -U admin -P admin raw 0x32 0x8f 0x02 0x01</pre>	

## PRELIMINARY

```
durmin raw 0x52 0x81 0x03 0x01  
ipmitool -I lanplus -H <bmc_ip> -U admin -P  
admin raw 0x32 0x83 0x03 0x01  
ipmitool -I lanplus -H <bmc ip> -U admin -P  
admin raw 0x32 0x83 0x04 0x01
```

## Upgrading the firmware of the BMC using the Web UI

**NOTICE**

Do not use, this feature may render the server unrecoverable.  
This feature is deprecated and will be removed in future firmware release.

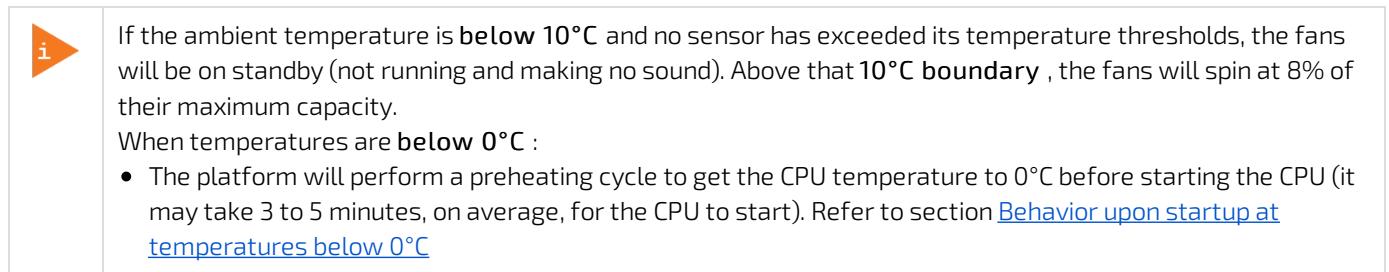
# Platform cooling and thermal management

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

## Table of contents

- [Thermal management](#)
- [Behavior upon startup at temperatures below 0°C](#)
- [Default temperature thresholds](#)

The ME1100 platform can operate within an ambient temperature range of -40°C to +65°C.



## Thermal management

The thermal 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 according to a PID algorithm. The temperature sensors are aggregated to provide an input value to the system temperature PID regulator, which provides a speed command for the fans.

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 (noted "OS reported" in the figure below) and then reported to the BMC. As such, the PCIe add-in card temperature, as well as the M.2 and SFP temperatures, can be reported to the BMC by the customer application and considered by the fan speed regulator in its computation for thermal management function.

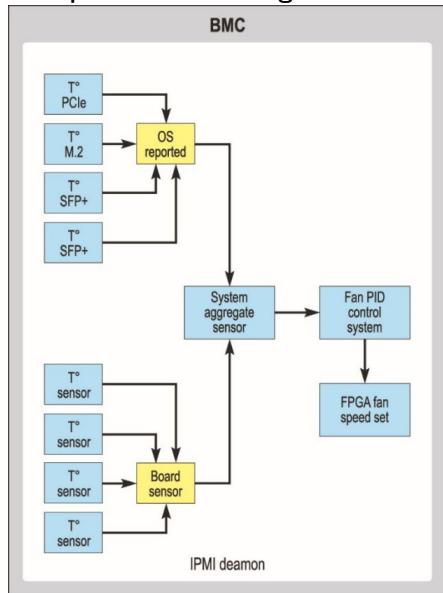
### Relevant sections:

[Managing customer added sensors](#)

[Sensor list](#)

[Interpreting sensor data](#)

### Temperature management



CP0212

# Behavior upon startup at temperatures below 0°C

Relevant section:

[Platform components](#)

When the platform is started at temperatures below 0°C:

- An internal heating element preheats the CPU prior to the board power on.
  - Platform is preheating:
    - Slow blink of the blue ID LED
    - Green Power LED off
- Once the CPU temperature reaches or exceeds 0°C, the CPU is powered on.
  - BMC executing an identification request:
    - Normal blink of the blue ID LED
    - Any state on the green Power LED
  - Server activation is complete:
    - Blue ID LED off
    - Rapid blink of the green Power LED

## Default temperature thresholds

Refer to [Monitoring sensors](#) for a list of methods to monitor temperature of sensors and means to configure user defined threshold values.

Sensor involved in platform cooling	Upper Non-Critical threshold
Temp CPU	70°C
Temp DIMM A	74°C
Temp DIMM B	74°C
Temp Inlet	54°C
Temp BMC	74°C
Temp Vcore	94°C
Temp Cortina	69°C
Temp NTC	74°C
Temp PCIe	User defined
Temp M.2	User defined
Temp SFP1	User defined
Temp SFP2	User defined

## Application ready indication via power LED

This section describes how to configure the power LED to indicate that the application is ready.

### NOTES:

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

## Prerequisites

1.	An OS is installed.
2.	An access to the OS is required. Refer to <a href="#">Accessing the operating system of a server</a> .
3.	The OS App. Ready Led Control BIOS option must be set to Disabled. Refer to <a href="#">Basic BIOS option configuration</a> .

## Example in C

The value 0x01 must be written to the I/O register 0xA20 (byte wide).

```
#include <sys/io.h>

int main(void)
{
    iopl(3);
    outb(0x01, 0xa20);
    iopl(0);
    return 0;
}
```

## Troubleshooting

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

Children

- [Collecting diagnostics](#)
- [\[Content under creation\] Working with logs](#)
- [\[Content under creation\] Working with error messages](#)
- [\[Content under creation\] Networking issues](#)
- [Factory default](#)
- [\[Content under creation\] Troubleshooting fans](#)
- [\[Content under creation\] How to recover from an erroneous CTRL-C](#)
- [Support information](#)

# Collecting diagnostics

{This article explains how to generate system logs.}

Table of contents

- [Collecting FRU information](#)
  - [Collecting FRU information using the BMC Web UI](#)
  - [Collecting FRU information using IPMI](#)
- [Collecting the firmware version](#)
  - [Collecting the firmware version using the BMC Web UI](#)
  - [Collecting the firmware version using IPMI](#)
- [Collecting the system event logs](#)
  - [Collecting the system event logs using the BMC Web UI](#)
  - [Collecting the system event logs using IPMI](#)

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

- [FRU information](#)
- [Firmware version](#)
- [System event log](#)

Collecting all this data beforehand can accelerate the process.

## Collecting FRU information

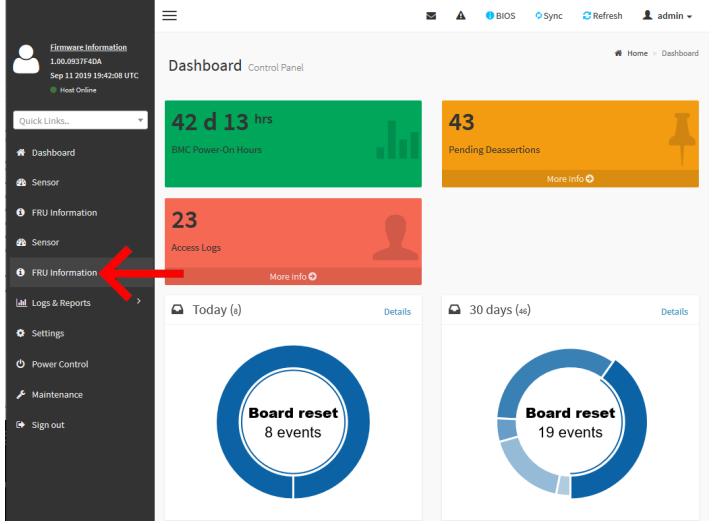
FRU information can be collected:

- Using the [BMC Web UI](#)
- Using [IPMI](#)

### Collecting FRU information using the BMC Web UI

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

## PRELIMINARY

Step_1	Access the BMC Web UI of the server.																																	
Step_2	Select <b>FRU Information</b> from the left side menu.  																																	
Step_3	The FRU information is displayed.  <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;"><b>Chassis Information</b></td> <td style="width: 33%; padding: 5px;"><b>Board Information</b></td> <td style="width: 33%; padding: 5px;"><b>Product Information</b></td> </tr> <tr> <td>Chassis Information Area Format Version</td> <td>Board Information Area Format Version</td> <td>Product Information Area Format Version</td> </tr> <tr> <td>Chassis Type : Rock Mount Chassis</td> <td>Language :</td> <td>Language :</td> </tr> <tr> <td>Chassis Part Number : [xxxx-xxxx]</td> <td>Manufacture Date Time : [Wed Mar 28 16:04:00 2018]</td> <td>Product Manufacturer : Kontron</td> </tr> <tr> <td>Chassis Serial Number : [xxxxxxxx]</td> <td>Board Manufacturer : Kontron</td> <td>Product Name : [ProductName]</td> </tr> <tr> <td>Chassis Extra : [ProductName]</td> <td>Board Product Name : [ProductName]</td> <td>Product Part Number : [xxxx-xxxx]</td> </tr> <tr> <td></td> <td>Board Serial Number : [xxxxxxxxxxxx]</td> <td>Product Version :</td> </tr> <tr> <td></td> <td>Board Part Number : [xxxx-xxxx]</td> <td>Product Serial Number : [xxxxxxxxxxxx]</td> </tr> <tr> <td></td> <td>FRU File ID : FRU-[ProductName]-[XX]</td> <td>Asset Tag :</td> </tr> <tr> <td></td> <td>Board Extra : MAC-[Base MAC address]/[Total MAC used]</td> <td>FRU File ID : FRU-[ProductName]-[XX]</td> </tr> <tr> <td></td> <td></td> <td>Product Extra : MAC-[Base MAC address]/[Total MAC used]</td> </tr> </table>	<b>Chassis Information</b>	<b>Board Information</b>	<b>Product Information</b>	Chassis Information Area Format Version	Board Information Area Format Version	Product Information Area Format Version	Chassis Type : Rock Mount Chassis	Language :	Language :	Chassis Part Number : [xxxx-xxxx]	Manufacture Date Time : [Wed Mar 28 16:04:00 2018]	Product Manufacturer : Kontron	Chassis Serial Number : [xxxxxxxx]	Board Manufacturer : Kontron	Product Name : [ProductName]	Chassis Extra : [ProductName]	Board Product Name : [ProductName]	Product Part Number : [xxxx-xxxx]		Board Serial Number : [xxxxxxxxxxxx]	Product Version :		Board Part Number : [xxxx-xxxx]	Product Serial Number : [xxxxxxxxxxxx]		FRU File ID : FRU-[ProductName]-[XX]	Asset Tag :		Board Extra : MAC-[Base MAC address]/[Total MAC used]	FRU File ID : FRU-[ProductName]-[XX]			Product Extra : MAC-[Base MAC address]/[Total MAC used]
<b>Chassis Information</b>	<b>Board Information</b>	<b>Product Information</b>																																
Chassis Information Area Format Version	Board Information Area Format Version	Product Information Area Format Version																																
Chassis Type : Rock Mount Chassis	Language :	Language :																																
Chassis Part Number : [xxxx-xxxx]	Manufacture Date Time : [Wed Mar 28 16:04:00 2018]	Product Manufacturer : Kontron																																
Chassis Serial Number : [xxxxxxxx]	Board Manufacturer : Kontron	Product Name : [ProductName]																																
Chassis Extra : [ProductName]	Board Product Name : [ProductName]	Product Part Number : [xxxx-xxxx]																																
	Board Serial Number : [xxxxxxxxxxxx]	Product Version :																																
	Board Part Number : [xxxx-xxxx]	Product Serial Number : [xxxxxxxxxxxx]																																
	FRU File ID : FRU-[ProductName]-[XX]	Asset Tag :																																
	Board Extra : MAC-[Base MAC address]/[Total MAC used]	FRU File ID : FRU-[ProductName]-[XX]																																
		Product Extra : MAC-[Base MAC address]/[Total MAC used]																																

## Collecting FRU information using IPMI

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

Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, access the FRU information. LocalServer_OSPrompt:~\$ ipmitool fru print	<pre>\$ ipmitool fru print FRU Device Description : Builtin FRU Device (ID 0) Board Mfg Date : [Wed Mar 28 16:04:00 2018] Board Mfg : Kontron Board Product : [ProductName] Board Serial : [xxxxxxxxxxxx] Board Part Number : [xxxx-xxxx] Board Extra : MAC-[Base MAC address]/[Total MAC used] Board Extra : MAC-[Base MAC address]/[Total MAC used] Product Manufacturer : Kontron Product Name : [ProductName] Product Part Number : [xxxx-xxxx] Product Version : Product Serial : [xxxxxxxxxxxx]</pre>
--------	--	---

## Collecting the firmware version

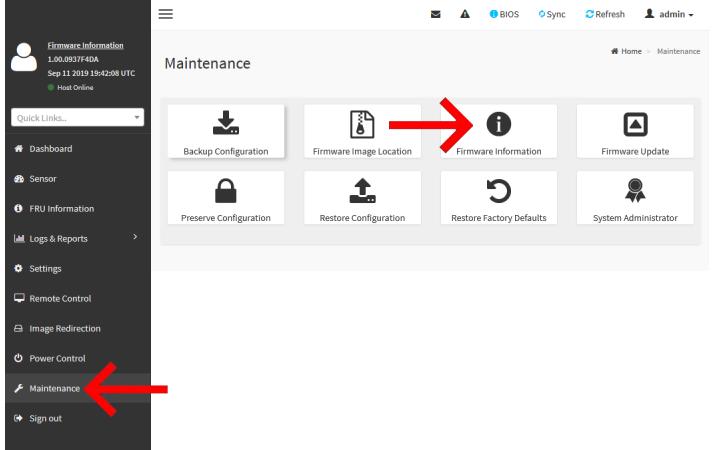
The firmware version can be collected:

- Using the [BMC Web UI](#)
- Using [IPMI](#)

### Collecting the firmware version using the BMC Web UI

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

## PRELIMINARY

Step_1	Access the BMC Web UI of the server.
Step_2	<p>From the left side menu, select <b>Maintenance</b> and then <b>Firmware Information</b>.</p> 
Step_3	The firmware version is displayed.

### Collecting the firmware version using IPMI

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

Step_1	<p>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, access the firmware information.</p> <pre>LocalServer_OSPrompt:~\$ ipmitool hpm check</pre>	<pre>\$ ipmitool hpm check PICMG HPM.1 Upgrade Agent 1.0.8: ----- Target Information----- Device Id      : 0x20 Device Revision : 0x1 Product Id     : 0x2722 Manufacturer Id : 0x3a98 (Kontron)  -----   ID   Name                      Versions                                   Active        Backup       --- --- --- --- --- --- --- ---    *0   BIOS            2.20 093694DD   ---.---     *1   FPGA            2.02 0800AD12   ---.---     *2   BOOT            12.00 00000000   ---.---     *3   APP             0.01 09369C38   ---.---   ----- (*) Component requires Payload Cold Reset</pre>
--------	--	--

### Collecting the system event logs

System event logs can be collected:

- Using the [BMC Web UI](#)
- Using [IPMI](#)

# PRELIMINARY

## Collecting the system event logs using the BMC Web UI

### Accessing the system event log

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

Step_1	Access the BMC Web UI of the server.	
Step_2	Select <b>Logs &amp; Reports</b> from the left side menu.	
Step_3	Select <b>IPMI Event Log</b> from the dropdown menu.	
Step_4	The system event log is displayed.	
Step_5	Click on an event and collect the following information: 1. Event ID 2. Associated sensor 3. Description 4. Time asserted	<p>1. ID: 16 Board reset sensor of type system_boot_or_restart_initiated 02 hours ago asserted on Thursday, October 3rd 2019, 8:58:47 am</p> <p>2. ID: 16 Board reset sensor of type system_boot_or_restart_initiated 02 hours ago asserted on Thursday, October 3rd 2019, 8:58:47 am</p> <p>3. ID: 16 Board reset sensor of type system_boot_or_restart_initiated 02 hours ago asserted on Thursday, October 3rd 2019, 8:58:47 am</p> <p>4. ID: 16 Board reset sensor of type system_boot_or_restart_initiated 02 hours ago asserted on Thursday, October 3rd 2019, 8:58:47 am</p>

### Downloading the system event log

## PRELIMINARY

<p><b>Step_1</b> In the Event Log menu, select Download Event Logs .</p>	
--	--

### Collecting the system event logs using IPMI

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

<p><b>Step_1</b> From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, access the system event log information .</p> <pre>LocalServer_OSPrompt:~\$ ipmitool sel</pre>	<pre>\$ ipmitool sel SEL Information Version      : 1.5 (v1.5, v2 compliant) Entries      : 52 Free Space   : 64566 bytes Percent Used : 1% Last Add Time: 1999-12-31 14:00:17 EST Last Del Time: Not Available Overflow     : false Supported Cmds: 'Delete' 'Partial Add' 'Reserve' 'Get Alloc Info' # of Alloc Units: 3639 Alloc Unit Size: 18 # Free Units  : 3587 Largest Free Blk: 3587 Max Record Size: 1</pre>
<p><b>Step_2</b> Access the system event log list.</p> <pre>LocalServer_OSPrompt:~\$ ipmitool sel elist</pre>	<pre>\$ ipmitool sel elist 1   2019-09-12   06:07:24 EDT   Event Logging Disabled BMC SEL State   Log area reset/cleared 2   2019-09-12   06:13:45 EDT   Temperature Temp CPU   Upper Critical going high   Asserted     Reading 34 &gt; Threshold 9 degrees C 3   2019-09-12   06:13:46 EDT   Platform Alert Health Status     Asserted 4   2019-09-12   06:13:46 EDT   Temperature Temp CPU   Upper Critical going high   Deasserted   Reading 34 &lt; Threshold 9 degrees C 5   2019-09-12   06:14:25 EDT   Platform Alert Health Status     Asserted 6   2019-09-12   06:26:45 EDT   Temperature Temp PCIe   upper Critical going high   Asserted     Reading 99 &gt; Threshold 99 degrees C 7   2019-09-12   06:26:46 EDT   Platform Alert Health Status     Asserted 8   2019-09-12   06:31:15 EDT   Platform Alert Health Status     Asserted 9   2019-09-12   06:31:49 EDT   Platform Alert Health Status     Asserted a   2019-09-12   06:34:30 EDT   Platform Alert Health Status     Asserted b   2019-09-12   06:54:49 EDT   Platform Alert Health Status     Asserted</pre>
<p><b>Step_3</b> Collect the following information for the specified event:</p> <ul style="list-style-type: none"> <li>• Event ID - 1st column</li> <li>• Time asserted - 2nd and 3rd column</li> <li>• Associated sensor - 4th column (optional)</li> <li>• Description - 5th column</li> </ul>	

# Factory default

{This article provides detailed instructions to reset the platform to factory default.}

Table of contents

- [Restoring default BIOS settings](#)
  - [Restoring default BIOS settings using the BIOS menu](#)
  - [Restoring default BIOS settings using IPMI](#)
  - [Restoring Default BIOS Settings Using Redfish](#)
- [Restoring Default BMC Settings](#)
  - [Restoring Default BMC Settings Using the BMC Web UI](#)
  - [Restoring Default BMC Settings Using Redfish](#)

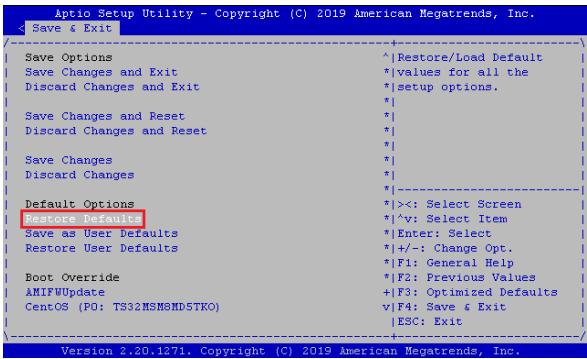
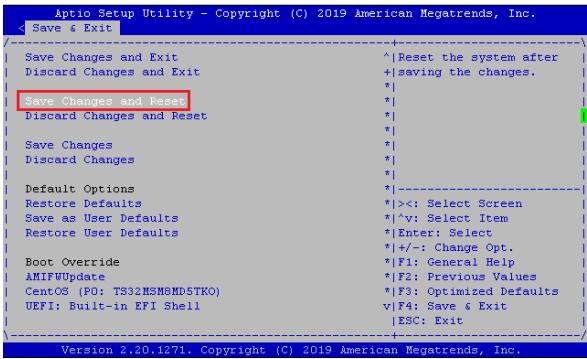
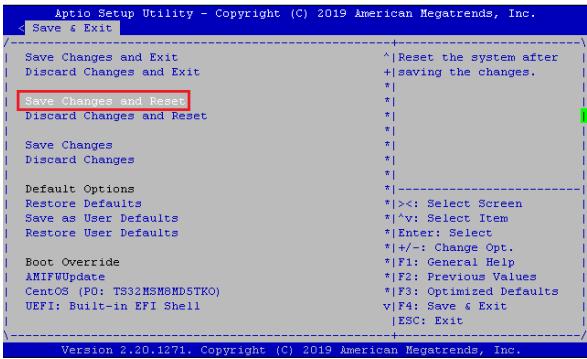
## Restoring default BIOS settings

The BIOS settings can be reset to factory default:

- Using the [BIOS menu](#)
- Using [IPMI](#)
- Using [Redfish](#)

### Restoring default BIOS settings using the BIOS menu

Refer to [Accessing the BIOS](#) for access instruction.

Step_1	Access the BIOS setup menu.	
Step_2	Access the Save & Exit menu and select Restore Defaults.	
Step_3	Select Save Changes and Reset .	
Step_4	Wait for the system to reset. The BIOS settings should have been reset to default values.	

### Restoring default BIOS settings using IPMI

The following procedures will be executed using the [Accessing a BMC on an ME module using IPMI \(KCS\)](#) method, operations could also be performed using IOL ([Accessing a BMC using IPMI over LAN \(IOL\)](#)). To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT\_IP] -U [IPMI user name] -P [IPMI password] .

## PRELIMINARY

Step_1	Restore default settings. LocalServer_OSPrompt:~\$ ipmitool chassis bootdev none clear-cmos=yes	<b>\$ ipmitool chassis bootdev none clear-cmos=yes Set Boot Device to none</b>
Step_2	Perform a platform reset. The BIOS settings should have been resetted to default values. LocalServer_OSPrompt:~\$ ipmitool chassis power reset <b>NOTE:</b> This step needs to be done within 1 minute after the IPMI command has been sent. Otherwise, the BMC will automatically clear the "bootdev" command.	<b>\$ ipmitool chassis power reset Chassis Power Control: Reset</b>

## Restoring Default BIOS Settings Using Redfish

Refer to [Accessing the BIOS using Redfish](#) for access instructions.

Step_1	Restore the BIOS menu default settings. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL] ]Systems/Self/Bios/Actions/Bios.ResetBios -X POST -d '{"ResetType":"Reset"}' -H "Content-Type: application/json"	<b>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Systems/Self/Bios/ Actions/Bios.ResetBios -X POST -d '{"ResetType":"Reset"}' -H "Content-Type: application/json"</b>
Step_2	Reset the platform. RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"ForceRestart"}' -H "Content-Type: application/json"	
Step_3	After reset, the BIOS settings should have been restored to default.	

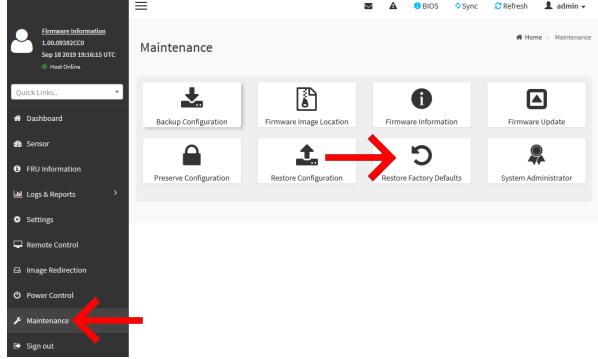
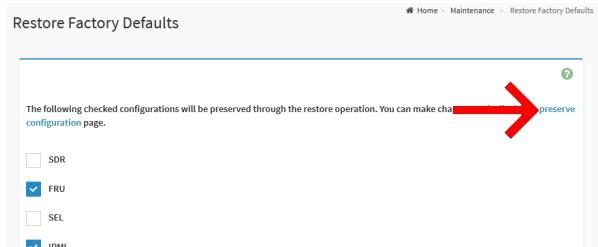
## Restoring Default BMC Settings

There are two ways to restore the BMC settings to factory default:

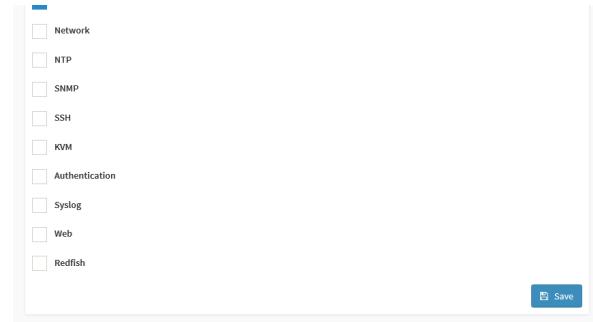
- [Using the Web UI](#)
- [Using Redfish](#)

### Restoring Default BMC Settings Using the BMC Web UI

Refer to [Accessing a BMC on an ME1100](#) for access instructions.

Step_1	Access the BMC Web UI of the server.	
Step_2	From the left side menu, select <b>Maintenance</b> and then <b>Restore Factory Defaults</b> .	
Step_3	If necessary, click on <b>preserve configuration</b> to change the list of unaffected configurations.	

# PRELIMINARY



Step_4	<p>Modify the list of preserved configurations as required. Click on <b>Save</b> and then <b>Factory Defaults</b> to return to the previous menu.</p>	
Step_5	<p>Click on the <b>Save</b> button.</p>	
Step_6	<p>Confirm the factory default restoration by clicking on <b>OK</b>.  <b>NOTE:</b> The platform will reset.</p>	

## Restoring Default BMC Settings Using Redfish

Refer to [Accessing a BMC on an ME1100](#) for access instructions.

## PRELIMINARY

Step_1	<p>Restore the default BMC settings.</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Managers/Actions/RedfishDBReset -X POST -d '{"FactoryResetType":"ResetAll"}' -H "Content-Type: application/json"   jq</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Managers/Self/Actions/RedfishDBReset -X POST -d '{"FactoryResetType":"ResetAll"}' -H "Content-Type: application/json"   jq {   "@Message.ExtendedInfo": [     {       "Message": "#Message.v1_0_5.Message",       "MessageId": "AniDom.1.0.0.webServerRestarting",       "Resolution": "Wait a few seconds before sending additional requests.",       "Severity": "Ok"     }   ] }</pre>
Step_2	<p>Verify the power state. Wait for the power state to be On .</p> <pre>RemoteComputer_OSPrompt:~\$ curl -k -s [ROOT_URL]Chassis/Self   jq .PowerState</pre>	<pre>\$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self -H "Content-Type: application/json"   jq .PowerState "On"</pre>
Step_3	<p>After reset, the BMC settings should have been restored to their default values.</p>	

## (WiP) - Restoring Default BIOS Settings Using the JP1 Connector

- Using the [JP1 connector](#) (not recommended – to use as a last resort)

### Restoring Default BIOS Settings Using the JP1 Connector

**NOTE:** This method is not recommended and should be used as a last resort if other methods did not work properly. Make sure to be aware of the risks and the precautions to ensure the platform's health.



#### ESD sensitive device!

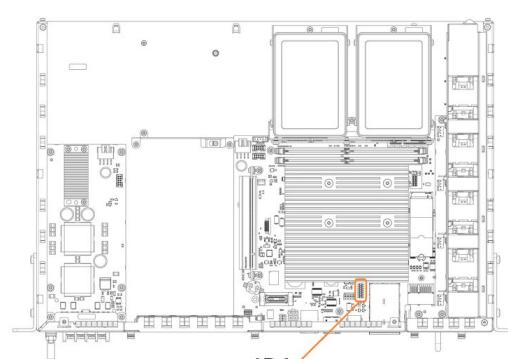
This equipment is sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.



When handling components, follow the precautions described in section [ESD protections](#).



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

Step_1	Power down the platform and remove the power cables. Refer to <a href="#">Platform power management</a> .																
Step_2	Open the enclosure. Refer to <a href="#">Component installation and assembly</a> .																
Step_3	Place a jumper between pins 11 and 12 of the JP1 connector.																
	 <table border="1" data-bbox="1285 1123 1444 1414"> <thead> <tr> <th colspan="2">Pinout</th> </tr> </thead> <tbody> <tr> <td>1</td><td>2</td></tr> <tr> <td>3</td><td>4</td></tr> <tr> <td>5</td><td>6</td></tr> <tr> <td>7</td><td>8</td></tr> <tr> <td>9</td><td>10</td></tr> <tr> <td>11</td><td>12</td></tr> <tr> <td>13</td><td>14</td></tr> </tbody> </table>	Pinout		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Pinout																	
1	2																
3	4																
5	6																
7	8																
9	10																
11	12																
13	14																
Step_4	Reconnect the power cables. Refer to <a href="#">Cabling</a> .																
Step_5	Power up ME1100 and wait for the OS to boot. Refer to <a href="#">Platform power management</a> . <b>NOTE:</b> BIOS will only reset settings to factory default right before the OS boots.																
Step_6	Power down the platform and remove the power cables. Refer to <a href="#">Platform power management</a> .																
Step_7	Remove the jumper between pins 11 and 12 of the JP1 connector.																
Step_8	Close the enclosure. Refer to <a href="#">Component installation and assembly</a> .																
Step_9	Reconnect the power cables.																
Step_10	Power up ME1100 Refer to <a href="#">Platform power management</a> . The BIOS settings should be restored to factory default.																

## Support information

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

---

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

- By phone: 1-888-835-6676
- By email: [support-kci@kontron.com](mailto:support-kci@kontron.com)
- Via the websites: [www.symkloud.com](http://www.symkloud.com) and [www.kontron.com](http://www.kontron.com)

## Reference guides

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

---

# Supported IPMI commands

Table of contents

- [Application commands](#)
  - [IPM device commands](#)
  - [Watchdog timer commands](#)
  - [BMC device and messaging commands](#)
  - [IPMI 2.0 specific commands](#)
  - [Chassis 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](#)
  - [IPM device commands](#)
  - [Serial over LAN commands](#)
- [AMI commands](#)
  - [AMI restore factory default settings command](#)
- [Kontron OEM commands](#)

## Application commands

### IPM device commands

## PRELIMINARY

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

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

### Watchdog timer commands

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

### BMC device and messaging commands

## PRELIMINARY

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

### IPMI 2.0 specific commands

## PRELIMINARY

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

### Chassis commands

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

### Bridge commands

# PRELIMINARY

## B Bridge management commands

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

## Bridge discovery commands

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

## Bridging commands

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

## Bridge event commands

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

## Sensor event commands

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

## Storage commands

### FRU information commands

## PRELIMINARY

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

### SDR repository commands

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

### SEL device commands

## PRELIMINARY

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

## Transport commands

### IPM device commands

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

### Serial over LAN commands

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

## AMI commands

### AMI restore factory default settings command

## PRELIMINARY

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

## Kontron OEM commands

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

NOTE: M/O = Mandatory/Optional

## Document symbols and acronyms

---

### Symbols

The following symbols are used in Kontron documentation.

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

	<b>Electric Shock!</b> This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of them. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material. Please also refer to the "High-Voltage Safety Instructions" portion below in this section.
---	--

	<b>ESD Sensitive Device!</b> 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.
	<b>HOT Surface!</b> Do NOT touch! Allow to cool before servicing.

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

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

### Acronyms

For a complete list of acronyms used in Kontron documentation, go to: [LINK TO COME](#).

# Safety and regulatory information

## Table of contents

- [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](#)

<b>NOTICE</b>	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

<b>WARNING</b>	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.
----------------	---

	<b>ESD sensitive device!</b> This equipment is sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.
---	---

### Elevated operating ambient temperature

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

### Reduced air flow

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

### Mechanical loading

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

### CE mark

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

## PRELIMINARY

### Waste electrical and electronic equipment directive

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

WEEE directive logo



### General power safety warnings and cautions

# PRELIMINARY



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



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.



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

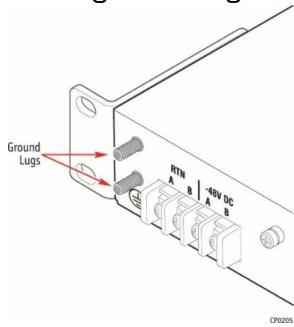
All of the following conditions must be met:

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

## Reliable earth-grounding

Always maintain reliable grounding of rack-mounted equipment.

## Earth ground lug location



## Regulatory specifications

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

# PRELIMINARY

## Safety compliance

USA/Canada	This product is marked cCSAus.
Europe	This product complies with the Low Voltage Directive, 2014/35/EU and EN 62368-1.
International	This product has a CB report and certificate to IEC 60950-1 and IEC 62368-1.

## Electromagnetic compatibility

USA/Canada	This product meets FCC Part 15/ICES-003 Class A. It is designed to meet GR-1089 and GR-63.
Europe	This product complies with the Electromagnetic Compatibility Directive 2014/30/EU and EN 300 386. The GPS version complies with Radio Equipment Directive 2014/53/EU, EN 301 489-1 and EN 303 413.
International	This product complies with CISPR 32 Class A and CISPR 35.

## 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](https://www.kontron.com/support-and-services/rma/canada/standard_warranty_policy_canada.pdf).

### Disclaimer

All data is for information purposes only and not guaranteed for legal purposes. Subject to change without notice. Information in this document has been carefully checked and is believed to be accurate; however, no responsibility is assumed for inaccuracies. All brand or product names are trademarks or registered trademarks of their respective owners.

### 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](mailto:support-na@kontron.com)
- Via the website: [www.kontron.com](http://www.kontron.com)

### Customer service

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

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