

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

COMPUTING

MaxCore™ MC3000 Platform

Installation and Use

P/N: 6806800T88K

April 2018

ARTESYN™
EMBEDDED TECHNOLOGIES

Downloaded from Arrow.com.

© Copyright 2018 Artesyn Embedded Technologies, Inc.

All rights reserved.

Trademarks

Artesyn Embedded Technologies, Artesyn and the Artesyn Embedded Technologies logo are trademarks and service marks of Artesyn Embedded Technologies, Inc. All other names and logos referred to are trade names, trademarks, or registered trademarks of their respective owners. © 2018 Artesyn Embedded Technologies, Inc. All rights reserved. For full legal terms and conditions, please visit www.artesyn.com/legal.

Notice

While reasonable efforts have been made to assure the accuracy of this document, Artesyn assumes no liability resulting from any omissions in this document, or from the use of the information obtained therein. Artesyn reserves the right to revise this document and to make changes from time to time in the content hereof without obligation of Artesyn to notify any person of such revision or changes.

Electronic versions of this material may be read online, downloaded for personal use, or referenced in another document as a URL to an Artesyn website. The text itself may not be published commercially in print or electronic form, edited, translated, or otherwise altered without the permission of Artesyn.

It is possible that this publication may contain reference to or information about Artesyn products (machines and programs), programming, or services that are not available in your country. Such references or information must not be construed to mean that Artesyn intends to announce such Artesyn products, programming, or services in your country.

Limited and Restricted Rights Legend

If the documentation contained herein is supplied, directly or indirectly, to the U.S. Government, the following notice shall apply unless otherwise agreed to in writing by Artesyn.

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data clause at DFARS 252.227-7013 (Nov. 1995) and of the Rights in Noncommercial Computer Software and Documentation clause at DFARS 252.227-7014 (Jun. 1995).

Contact Address

Artesyn Embedded Technologies

Marketing Communications

2900 S. Diablo Way, Suite 190

Tempe, Arizona 85282

Downloaded from Arrow.com.

Contents

About this Manual 11

Safety Notes 17

Sicherheitshinweise 29

1 Product Documentation Overview 41

2 System Overview 43

2.1 System Views and Components 43
2.1.1 PCIe Card Slots 45
2.1.2 Processor Subsystem 45
2.1.3 IO Panel 46
2.1.3.1 Disk Drive Bays 47
2.1.4 AC and DC Power Supply Modules 47
2.1.5 Fan Modules 47
2.1.6 Air Filter and Front Bezel 47
2.2 System Management 48
2.3 Standard Compliances 49
2.4 Ordering Information 51

3 Site Preparation 53

3.1 Site Planning Considerations 53
3.1.1 Unpacking the System 53
3.1.2 Site and Installation Planning 54
3.2 Precautions 55
3.2.1 ESD Prevention 56
3.3 Requirements 57
3.3.1 Environmental Requirements 57
3.3.2 Power Requirements 60
3.4 Dimensions and Weight 62
3.5 Mounting Options 62
3.5.1 MaxCore Rackmount Slides Installation 64
3.6 Cooling Considerations 73

Downloaded from Arrow.com.

3.7 Acoustic Noise Control 74

4 FRU Installation 75

4.1 Installing and Removing PCIE Cards 75
4.2 Replacing AC Power Supply Units 78
4.3 Replacing DC Power Supply Units 81
4.4 Maintaining Air Filters 84
4.4.1 Replacing the Air Filter 85
4.4.2 Storing the Air Filters 86
4.5 Replacing Fan Modules 87
4.6 Installing Disk Drives into MaxCore Platform 91

5 Cooling Subsystem 97

5.1 Cooling Subsystem 97

6 System Installation 99

6.1 Before Installation 99
6.1.1 Tools Required 99
6.1.2 Torque Values 100
6.1.3 Type Label Location 100
6.2 Installation 101
6.2.1 Installing the System in a Rack 102
6.2.2 Grounding the System 105
6.2.3 Powering Up the System 106
6.2.3.1 AC System Startup Procedure 106
6.2.3.2 DC System Startup Procedure 109
6.3 Removal 112
6.3.1 Powering Down the System 112
6.3.2 Disconnecting the System from Power Feed 113
6.3.2.1 AC System Disconnection Procedure 114
6.3.2.2 DC System Disconnection Procedure 115
6.3.3 Removing the System 115

Downloaded from Arrow.com.

7 Operation and Maintenance 117

7.1 Remote Management via Board Management Controller 117
7.1.1 Copyright Notice 117
7.1.2 AMI MegaRAC® WEB GUI 118
7.1.2.1 Login Screen 119
7.1.3 Using MegaRAC SP-X 121
7.1.3.1 Quick Button and Logged-in User 121
7.1.3.2 Dashboard 122
7.1.3.3 Field Replaceable Unit Information 124
7.1.3.4 Server Health 126
7.1.3.5 Configuration Group 133
7.1.3.6 Remote Control 184
7.1.3.7 Maintenance 186
7.1.3.8 Firmware Update 188
7.1.3.9 MaxCore Chassis 194
7.1.3.10 Log Out 198
7.2 Serial Over LAN 198
7.2.1 SOL via IPMI 199
7.2.1.1 Configuring BIOS 199
7.2.1.2 Configuring OS 200
7.2.1.3 Establishing SOL to any System Host Micro Server Card 200
7.2.2 SOL via SSH 200
7.3 Remote KVM and Media 201
7.3.1 Invocation Procedure 201
7.3.2 Reference Guide 202
7.3.2.1 Video 203
7.3.2.2 Keyboard 204
7.3.2.3 Mouse 204
7.3.2.4 Options 206
7.3.2.5 Media 208
7.3.2.6 Keyboard Layout 210
7.3.2.7 Video Record 211
7.3.2.8 Power 213
7.3.2.9 Active Users 213
7.3.2.10 Help 213

Downloaded from Arrow.com.

7.3.2.11 Quick Buttons 213
7.4 OEM Commands 215
7.4.1 OEM Command Summary 215
7.4.2 shelfHost Configuration 216
7.4.2.1 Default shelfHost Configuration 217
7.4.2.2 Set shelfHost Configuration 217
7.4.2.3 Get shelfHost Configuration 218
7.4.3 Power Management 219
7.4.3.1 Set FRU Instance Power State 220
7.4.3.2 Get FRU Instance Power State 221
7.4.3.3 Set Chassis Power Policy 222
7.4.3.4 Get Chassis Power Policy 222
7.4.4 FRU UART Management 223
7.4.4.1 Set FRU Instance Serial Route 224
7.4.4.2 Get FRU Instance Serial Route 225
7.4.5 Configuring BMC Features 225
7.4.5.1 Set BMC Feature Configuration 226
7.4.5.2 Get BMC Feature Configuration 227
7.5 MaxCore Firmware Upgrade 227
7.5.1 Obtaining Revisions of Firmware Components 228
7.5.2 Upgrade Procedure 229
7.5.3 Troubleshooting 233
7.5.3.1 CPLD FW Upgrade Failed 234
7.5.3.2 BMC FW Upgrade Failed 234
7.5.3.3 BMC Cannot Be Accessed Via IP address 234
7.6 Modifying the BMC IP Address 234

A Troubleshooting 237

B Related Documentation 241

B.1 Artesyn Embedded Technologies - Embedded Computing Documentation 241
B.2 Related Specifications 242

Downloaded from Arrow.com.

List of Tables

Table 2-1 Standard Compliances 49
Table 2-2 Ordering Information 51
Table 3-1 Environmental Conditions 58
Table 3-2 Critical Temperature Limits 59
Table 3-3 AC System Power Requirements 60
Table 3-4 DC System Power Requirements 60
Table 3-5 Typical Power Consumption Values 61
Table 3-6 Dimensions and Weight of System and Components 62
Table 3-7 Components in Rail Kit 66
Table 6-1 Torque Values 100
Table 7-1 Login Page 119
Table 7-2 Logged-in User Information 122
Table 7-3 Dashboard 123
Table 7-4 FRU Information 125
Table 7-5 Event Log 130
Table 7-6 DNS Server Settings 135
Table 7-8 Local Media 139
Table 7-7 Advanced Media Settings 139
Table 7-9 Remote Media 141
Table 7-10 Mouse Mode Settings 142
Table 7-11 NCSI 143
Table 7-12 Network Settings 144
Table 7-13 Network Settings 147
Table 7-14 NTP Settings 148
Table 7-15 Remote Session 160
Table 7-16 SMTP Settings 166
Table 7-17 Upload SSL 170
Table 7-18 Generate SSL 171
Table 7-19 Generate SSL 173
Table 7-20 System and Audit Log Settings 175
Table 7-21 User Management 178
Table 7-22 Virtual Media 182
Table 7-23 Power Control and Status 185
Table 7-24 Synchronize Configuration 186
Table 7-25 System Administrator 187
Table 7-26 Firmware Update 190

Downloaded from Arrow.com.

Table 7-27 Dual Image Configuration 193
Table 7-28 shelfHost Configuration 195
Table 7-29 USB & SATA Configuration 197
Table 7-30 PCIe Configuration 198
Table 7-31 Video menu 203
Table 7-32 Keyboard menu 204
Table 7-33 Mouse menu 204
Table 7-34 Options menu 206
Table 7-35 Media menu 208
Table 7-36 Keyboard menu 210
Table 7-37 Video Record menu 211
Table 7-38 Power menu 213
Table 7-39 Quick buttons 213
Table 7-40 General OEM Command Structure 215
Table 7-41 OEM Command Summary 215
Table 7-42 Default shelfHost Configuration 217
Table 7-43 Set shelfHost Configuration Table 217
Table 7-44 Get shelfHost Configuration 218
Table 7-45 Set FRU Instance Power State 220
Table 7-46 Get FRU Instance Power State 221
Table 7-47 Set Chassis Power Policy 222
Table 7-48 Get Chassis Power Policy 222
Table 7-49 Set FRU Instance Serial Route 224
Table 7-50 Get FRU Instance Serial Route 225
Table 7-51 BMC watchdog configuration 226
Table 7-52 Set BMC Feature Configuration 226
Table 7-53 Get BMC Feature Configuration 227
Table B-1 Artesyn Embedded Technologies - Embedded Computing Publications 241
Table B-2 Related Specifications 242

Downloaded from Arrow.com.

List of Figures

Figure 2-1 MaxCore Front View 44
Figure 2-2 MaxCore Rear View 44
Figure 2-3 IO Panel 46
Figure 3-1 Rack Mounting Dimensions 64
Figure 3-2 Rack posts - 20” and 30” 64
Figure 3-3 EIA Rail Spacing 65
Figure 4-1 MaxCore PCIe Slots 76
Figure 4-2 Location of AuxPower Connectors in MaxCore System 77
Figure 6-1 Serial Number Label Location 100
Figure 6-2 Rack Mounting Dimensions 104
Figure 6-3 System’s Ground 105
Figure 7-1 Login Screen 119
Figure 7-2 Menu Bar 121
Figure 7-3 Logged-in User Information 121
Figure 7-4 Dashboard Screen 123
Figure 7-5 FRU Information Page 125
Figure 7-6 Server Health Menu 126
Figure 7-7 Sensor Readings 127
Figure 7-8 Widget 129
Figure 7-9 Event Log 130
Figure 7-10 System and Audit Logs - System Log Tab 132
Figure 7-11 System and Audit Logs - Audit Log Tab 132
Figure 7-12 Configuration Menu 133
Figure 7-13 DNS Server Settings 134
Figure 7-14 Image Redirection 138
Figure 7-15 Advanced Media Settings 138
Figure 7-16 NCSI Settings 143
Figure 7-17 Network Settings 144
Figure 7-18 NTP Settings 148
Figure 7-19 PEF Management - Event Filter 151
Figure 7-20 PEF Management - Alert Policy 155
Figure 7-21 PEF Management LAN Destination 158
Figure 7-22 Services Page 162
Figure 7-23 SMTP Settings 166
Figure 7-24 SSL Certificate Configuration 170
Figure 7-25 SSL Certificate Configuration - Generate SSL 171

Downloaded from Arrow.com.

Figure 7-26 SSL Certificate Configuration - View SSL 172
Figure 7-27 System and Audit Settings 175
Figure 7-28 System Firewall 177
Figure 7-29 User Management 178
Figure 7-30 Virtual Media 182
Figure 7-31 Console Redirection 184
Figure 7-32 Chassis Power Control and Status 185
Figure 7-33 Firmware Update 189
Figure 7-34 Upload Firmware 191
Figure 7-35 Section Based Firmware Update 192
Figure 7-36 Dual Image Configuration 193
Figure 7-37 MaxCore Chassis Menu 195
Figure 7-38 shelfHost Configuration 195
Figure 7-39 USB & SATA Configuration 196
Figure 7-40 Virtual Media 209
Figure 7-41 Video Record Settings Page 212
Figure 7-42 Dual Image Configuration 230
Figure 7-43 Firmware Update - Upgrade 231

Downloaded from Arrow.com.

Overview of Contents

This manual is divided into the following chapters and appendices.

- *Safety Notes* provides the safety information that should be observed while operating the product.
- *Sicherheitshinweise* provides a German translation of the chapter, "Safety Notes".
- *Product Documentation Overview* provides a brief description of the product and the list of manuals that need to referred while working on the product.
- *System Overview* provides an overview of the features of the MaxCore system and lists order numbers.
- *Site Preparation* provides site planning considerations, describes requirements and conditions.
- *FRU Installation* describes how to install and replace PCIe cards, fan modules, PSUs, and air filters.
- *Cooling Subsystem* provides information about cooling management.
- *System Installation* describes how to install, remove, and run the MaxCore system.
- *Operation and Maintenance* provides Remote Management via Base Management Controller, Serial Over LAN, and OEM Commands related information.
- *Related Documentation* lists related documentation and specifications.

Abbreviations

This document uses the following abbreviations:

Abbreviation	Definition
AMQP	Advanced Message Queue Protocol
ANSI	American National Standards Institute
AWG	American Wire Gauge
BMC	Baseboard Management Controller
CISPR	Comité International Spécial des Perturbations Radioélectriques

Downloaded from Arrow.com.

Abbreviation	Definition
COTS	Commercial off-the-Shelf
CPLD	Complex Programmable Logic Device
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module
DNS	Domain Name System
DPDK	Data Plane Development Kit
ECC	Error Correcting Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMV	Elektromagnetische Vertraeglichkeit
EN	European Norm
ESD	Electrostatic Discharge
ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
FCU	Firmware Upgrade Utility
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
IEC	International Electric Code
IEEE	Institute of Electrical and Electronics Engineers
iSCSI	Internet Small Computer System Interface
JRE	Java Runtime Environment
KVM	Kernel Virtual Machine
LNC	Lower Non-Critical
LNR	Lower Non-Recoverable
LC	Lower Critical
IPMI	Intelligent Platform Management Interface
MCCS	MaxCore Configuration Service
ME	Management Engine

Downloaded from Arrow.com.

Abbreviation	Definition
NEBS	Network Equipment Building System
NEC	National Electric Code
NFS	Network File System
NCSI	Network Controller Sideband Interface
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OSP	Outside Plant
OTP	Over Temperature Protection
OVP	Over Voltage Protection
PCI	Peripheral Component Interconnect
PCI-E or PCIe	PCI Express
PCI-SIG	PCI Special Interest Group
PEF	Platform Event Filtering
PSU	Power Supply Unit
QEMU	Quick Emulator
RMCP	Remote Management Control Protocol
RoHS	Restriction of Certain Hazardous Substances
SATA	Serial ATA
SCSI	Small Computer System Interface
SELV	Safety Extra Low Voltage
SGA	Shelf Geographical Address
SMTP	Simple Mail Transfer Protocol
SOL	Serial Over LAN
SSF	System Services Framework
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Shielded Twisted Pair
TFTP	Trivial File Transfer Protocol

Downloaded from Arrow.com.

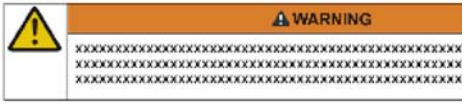
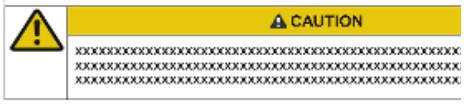
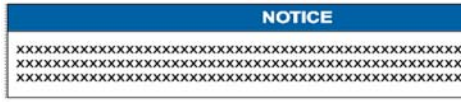
Abbreviation	Definition
TNV	Telecommunications Network Voltage
TPE	Twisted-Pair Ethernet
TPM	Trusted Platform Module
UL	Underwriters Laboratories
UC	Upper Critical
UNR	Upper Non-Recoverable
UNC	Upper Non-Critical
VCCI	Voluntary Control Council for Interference
VEB	Virtual Ethernet Bridging
WEEE	Waste from Electrical and Electronic Equipment

Conventions

The following table describes the conventions used throughout this manual.

Notation	Description
0x00000000	Typical notation for hexadecimal numbers (digits are 0 through F), for example used for addresses and offsets
0b0000	Same for binary numbers (digits are 0 and 1)
bold	Used to emphasize a word
`Screen`	Used for on-screen output and code related elements or commands in body text
`Courier + Bold`	Used to characterize user input and to separate it from system output
Reference	Used for references and for table and figure descriptions
File > Exit	Notation for selecting a submenu
<text>	Notation for variables and keys
[text]	Notation for software buttons to click on the screen and parameter description

Downloaded from Arrow.com.

Notation	Description
...	Repeated item for example node 1, node 2, ..., node 12
. . .	Omission of information from example/command that is not necessary at the time being
..	Ranges, for example: 0..4 means one of the integers 0,1,2,3, and 4 (used in registers)
|	Logical OR
	Indicates a hazardous situation which, if not avoided, could result in death or serious injury
	Indicates a hazardous situation which, if not avoided, may result in minor or moderate injury
	Indicates a property damage message
	No danger encountered. Pay attention to important information

Downloaded from Arrow.com.

Summary of Changes

This manual has been revised and replaces all prior editions.

Part Number	Date	Description
6806800T88K	April 2018	Updated Chapter 7, *Operation and Maintenance, on page 117*. Removed the chapter PCIE-7410 Processor Subsystem.
6806800T88J	September 2017	Updated chapter PCIE-7410 Processor Subsystem and section *Obtaining Revisions of Firmware Components* on page 228. Added a section Upgrading Linux. Added a command for aCPU power policy in sections *Set FRU Instance Power State* on page 220 and *Get FRU Instance Power State* on page 221.
6806800T88H	April 2017	Updated company address information. Updated the chapter *Product Documentation Overview* on page 41.
6806800T88G	December 2016	Updated a section Building your own Linux Kernel.
6806800T88F	October 2016	Added new section *Remote KVM and Media* on page 201, Updated Table 3-1 on page 58. Updated the section *Serial Over LAN* on page 198.
6806800T88E	August 2016	Updated application note related description in Chapter 1, *Product Documentation Overview, on page 41* and also updated Appendix B, *Related Documentation, on page 241*.
6806800T88D	July 2016	Incorporated out-of-box-experience feedback comments.
6806800T88C	April 2016	Added a section *MaxCore Rackmount Slides Installation* on page 64.
6806800T88B	March 2016	Updated the section *Serial Over LAN*. Updated trademarks section and also re-branded the header image.
6806800T88A	January 2016	Initial version

Downloaded from Arrow.com.

Safety Notes

This section provides warnings that precede potentially dangerous procedures throughout this manual. Instructions contained in the warnings must be followed during all phases of operation, service, and repair of this equipment. You should also employ all other safety precautions necessary for the operation of the equipment in your operating environment. Failure to comply with these precautions or with specific warnings elsewhere in this manual could result in personal injury or damage to the equipment.

Artesyn intends to provide all necessary information to install and handle the product in this manual. Because of the complexity of this product and its various uses, we do not guarantee that the given information is complete. If you need additional information, ask your Artesyn representative.

The product has been designed to meet the standard industrial safety requirements. It must only be used in its specific area of office telecommunication industry, industrial control, and development. It must not be used in safety critical components, life supporting devices or on aircraft.

Only personnel trained by Artesyn or persons qualified in electronics or electrical engineering are authorized to install, remove or maintain the product. The information given in this manual is meant to complete the knowledge of a specialist and must not be used as replacement for qualified personnel.

Keep away from live circuits inside the equipment. Operating personnel must not remove equipment covers. Only factory authorized service personnel or other qualified service personnel may remove equipment covers for internal subassembly or component replacement or any internal adjustment.

Do not install substitute parts or perform any unauthorized modification of the equipment or the warranty may be voided. Contact your local Artesyn representative for service and repair to make sure that all safety features are maintained.

EMC

The product has been tested and found to comply with the limits for a Class A digital device in this system, pursuant to part 15 of the FCC Rules, EN 55022 Class A respectively. These limits are designed to provide reasonable protection against harmful interference when the product is operated in a commercial, business or industrial environment.

Downloaded from Arrow.com.

The product generates and uses radio frequency energy and, if not installed properly and used in accordance with this user's documentation, may cause harmful interference to radio communications. Operating the product in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense. To ensure proper EMC shielding, operate the system only with free slots populated with filler cards.

To ensure EMC protection use only shielded cables when connecting peripherals to assure that appropriate radio frequency emissions compliance is maintained. Installed PCIe cards must have the faceplates installed and all vacant slots in the shelf must be covered.

Grounding
If the product is not properly grounded, it may be damaged by electrostatic discharge.
Make sure that each of the system's parts contact the EMI gasket. The system contains gaskets at the shelf and module level.
The shelf is also fitted with ESD snaps for the use with conductive wrist straps. Please take care for proper ESD protection of the operator.

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Interference (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

The equipment is suitable for installation in a Common Bonding Network (CBN) or Isolated Bonding Network (IBN).

System Installation

System Damage
To avoid system damage verify that the system environment meets the environmental and power requirements given in this manual before installing the system.

Downloaded from Arrow.com.

Before you begin to set up and cable your new system, consider these guidelines:

- Installation codes: This unit must be installed in accordance with the National Electrical Code.
- Overcurrent protection: A readily accessible listed branch circuit overcurrent protective device must be incorporated into the building wiring. For appropriate AWG rating of the overcurrent protection device, see NEC Table 310.16 and other national regulations.
- The protective bonding conductor depends on your power distribution topology. Make sure that you use an appropriate protective bonding conductor regarding the rating of the branch circuit protection.
- Install the system safely. Make sure that cables and cords are out of the way.
- Make sure that the set-up is comfortable for users.

System Damage
WARNING: The intra-building port (s) of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port (s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

System Damage
Environmental contamination can impair system operation.
Locate the system in a stable area free of excess movement and jarring and free of dust, smoke, and electrostatic discharge (ESD). Make sure that the temperature does not exceed the operating temperature given in the environmental requirements in this manual and allow room for proper air flow for cooling.

Personal Injury or System Damage (For AC)
The system is supplied by AC mains primary voltage. This voltage is considered hazardous. Take appropriate precaution when cabling the system.

Downloaded from Arrow.com.

Personal Injury or System Damage (For DC)
The system is supplied by a TNV-2 voltage. This voltage is considered hazardous. Make sure that the power supply meets the relevant safety standards.
Ensure that TNV-2 is separated from dangerous voltages (mains) through double or reinforced insulation.

Personal Injury or System Damage
A top-heavy rack can topple over, causing damage to equipment and injury to personnel.
If your system is the only one in the rack, make sure to mount the system in the lowest part of the rack. If several systems are installed in one rack, start with the heaviest component at the bottom. If the rack is equipped with stabilizing devices, make sure that they are installed and extended so that the rack is secure. Then proceed to mount or service the system.

Personal Injury or System Damage
When pulling the system out of the rack, it can fall down and cause injuries.
Pull out the system cautiously.

Personal Injury
The system is heavy and improper handling may lead to muscle strain or back injury.
Have two people lift the system or use lifting aids and proper lifting techniques when handling the system. Do not use the handles on the fans or PSUs to lift the system.

System Damage
During the course of handling, shipping and assembly, pins, mounting screws, fans and other items can become loose or damaged.
Do not operate a damaged system, this can cause damage to devices that interfere with it.

Personal Injury
High leakage current can be hazardous and cause injury.

Downloaded from Arrow.com.

Locate the caution label near the grounding studs (may vary from system to system) and make an earth ground connection before connecting power to the PSU.



System Damage
Wrong jumper settings can make the system inoperable. Therefore, never change the settings of the jumpers.

Card Installation

Damage of Circuits
Electrostatic discharge and incorrect installation and removal of the product can damage circuits or shorten their life.
Before touching the product make sure that your are working in an ESD-safe environment or wear an ESD wrist strap or ESD shoes. Hold the product by its edges and do not touch any components or circuits.

Damage of System or Card
Installing a card in the wrong slot may cause card or system damage.
Only install PCIE cards in the designated slots.
Removing the card from the system while the system is powered up may damage the card.
Whenever removing the card from the system, power down system first. This does not apply to hot-swap cards.

Data Loss
The MaxCore system does not support hot swap of PCIE cards. Before opening the top cover of the system or before removing or inserting any PCIE card, make sure the system is powered off. Disconnect the system from any AC or DC power or at least turn the system board power (aka payload power) off through the Board Management Controller (BMC).

Downloaded from Arrow.com.

Card Malfunctioning
Incorrect card installation and removal can result in card malfunctioning.
Make sure the card is connected to the PCIe slot in the system.

Operation

System Overheating
Cooling Vents
Improper cooling can lead to card and system damage and may void the manufacturer's warranty.
To ensure proper cooling and undisturbed airflow through the system always operate the system in a horizontal position. Do not obstruct the ventilation openings at the front and rear of the system. Keep the fresh air intake at the bottom-front side of the chassis completely clear. Make sure that the fresh air supply is not mixed with hot exhaust from other devices. Make sure that all slots are populated with PCIE cards or filler cards.

Product Damage
High humidity and condensation on card surfaces causes short circuits.
Do not operate the system outside the specified environmental limits. Make sure the system is completely dry and there is no moisture on any surface before applying power. Do not start the system below 0 ºC.

Injury
Caution: The MaxCore system has 3 PSUs (three power connection feeds). All must be disconnected to de-energize the system. To reduce the risk of injury, disconnect the feeds when removing power from the system.

System Damage
Air Filters
Air contamination can pollute the air filter and obstruct the air intake of the system which may cause system overheating and component damage.

Downloaded from Arrow.com.

To guarantee proper airflow through the system the air filters have to be replaced at least every six months. Artesyn recommends to replace the air filters every 90 days. Filter replacement frequency depends on the environment the system is subjected to.
Because central offices vary in physical location and cleanliness, check your air filters every week after you first install your system. In a dusty environment, filter replacement may be required more often than in a cleaner environment. Check the filters frequently until you have a good idea of how often they must be replaced. Based on your findings, establish a regular replacement schedule and keep a log to record the date of each filter replacement.

Filter Frames
Wrong insertion may damage the frame or front panel.
The front panel including the air filter is mounted to the system by alignment pins and holding clips on both sides of the system. When mounting the filter frame to the shelf, pay attention to align it accurately.

This equipment is designed to permit the connection of the earthed conductor of the DC supply circuit to the earthing conductor at the equipment. If this connection is made, all of the following conditions must be met:

- This equipment shall be connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.
- 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 DC supply circuit and the earthing conductor, and also the point of earthing of the DC system. The DC system shall not be earthed elsewhere.
- The DC supply source shall be located within the same premises as this equipment.
- Switching or disconnecting devices shall not be in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

Downloaded from Arrow.com.

French translation: Cet appareil est conçu pour permettre le raccordement du conducteur relié à la terre du circuit d'alimentation c.c. au conducteur de terre de l'appareil. Pour ce raccordement, toutes les conditions suivantes doivent être respectées:

- Ce matériel doit être raccordé directement au conducteur de la prise de terre du circuit d'alimentation c.c. ou à une tresse de mise à la masse reliée à une barre omnibus de terre laquelle est raccordée à l'électrode de terre du circuit d'alimentation c.c.
- Les appareils dont les conducteurs de terre respectifs sont raccordés au conducteur de terre du même circuit d'alimentation c.c. doivent être installés à proximité les uns des autres (p.ex., dans des armoires adjacentes) et à proximité de la prise de terre du circuit d'alimentation c.c. Le circuit d'alimentation c.c. ne doit comporter aucune autre prise de terre.
- La source d'alimentation du circuit c.c. doit être située dans la même pièce que le matériel. - Il ne doit y avoir aucun dispositif de commutation ou de sectionnement entre le point de raccordement au conducteur de la source d'alimentation c.c. et le point de raccordement à la prise de terre.

System Overheating
If you set the fan speed manually through the Board Management Controller (BMC), constantly monitor the system temperature to prevent overheating.
While operating the system ensure that the environmental and power requirements are met.

Injuries or Short Circuits
To avoid damage or injuries, always check that there is no more voltage on the line that has been disconnected before continuing your work.

System Expansion

System Overload
To avoid an overload of the system check the total power consumption of all components installed (see the technical specification of the respective components). Ensure that any individual output current of any source stays within its acceptable limits (see the technical specification of the respective source).

Downloaded from Arrow.com.

Loss of Safety Compliance
Using of Additional Plug-in Cards
By using additional plug-in cards it may be possible that the system may become incompliant.
The system integrator has to ensure that the compliancy is guaranteed.

Power Feed

Personal Injury
Touching the power feed with metallic objects on your hands, wrists, or hanging from your neck may lead to severe injuries through electric shock and burning.
Do not wear any metallic attire or commodity on your hands, wrists, or hanging from your neck when working at the power feed or power input cables. Be extremely careful when you use electrically conductive tools near the PSUs.

Short Circuits or Personal Injury
Ensure that the power feeds you plan to remove or attach are powered off and cannot be switched on while you are working.
Ensure that all power input lines are not energized. Be careful with the tools used in order to prevent a short circuit.

Product Damage
Improper cabling damages your product.
Take extreme care not to connect the power cable in reverse polarity.

AC PSUs

Personal Injury
Hot PSUs may cause injury.
Allow the PSU to cool before servicing.

Downloaded from Arrow.com.

DC PSUs

Personal Injury
Hot PSUs may cause injury.
Allow the PSU to cool before servicing.

System Damage
Inserting or extracting the PSU with the power cable connected and inlet power active may damage the PSU or your system.
If the power cable is connected to the PSU, make sure the inlet power is switched off at the Power Distribution Unit (PDU) before you insert or extract a PSU.

PSU Damage
Operating the PSU while there is a permanent short circuit in the system may lead to PSU damage.
Make sure that there is no shortage in the system.

Fan Trays

System Damage
Insufficient cooling may damage the system.
The cooling system is designed to provide sufficient cooling with a single fan tray at work. However, under bad conditions or due to a failure of the remaining fans, the cooling capacity of a single fan tray may not suffice.
Avoid delays during fan replacement.

Fan Damage
When a fan tray is taken out of operation or is removed during a replacement procedure, the system manager will compensate for the loss by increasing the speed of the remaining fans. Turning on high speed for a long time may shorten the life of the fans and may exceed allowable acoustic noise limits.
Replace the fan tray without delays.

Downloaded from Arrow.com.

System Damage
Removing the single operating fan tray will lead to overheating very quickly.
Make sure that there is always one operating fan tray present in the system.

Personal Injury
Rotating Fans
Inserting tools or fingers into operational fans may cause injuries.
Keep clear of the fans as long as they are rotating.

Cabling

Personal Injury
The cabling should follow existing cable paths using existing or similar cable fastenings. Never change the system's cabling as delivered by Artesyn. Check proper function of the system after cabling extensions. To avoid injuries always ensure that cables are securely installed so that nobody can trip over them.

Personal Injury through Electric Shock
Touching contacts and cables during system operation can cause injuries through electric shock.
To avoid electric shock make sure that contacts and cables of the system cannot be touched while the system is operating. If in doubt concerning cabling, ask your local Artesyn representative.

Cable Damage
Folding the fiber cable damages the cable and inhibits the data transmission. Therefore, make sure you do not fold the cable.

Downloaded from Arrow.com.

RJ-45 Connector

System Damage
RJ-45 connectors on the I/O module of the system or on PCIE cards are either twisted-pair Ethernet (TPE) or E1/T1/J1 network interfaces. Connecting an E1/T1/J1 line to an Ethernet connector may damage your system.

- Make sure that TPE connectors near your working area are clearly marked as network connectors.
- Verify that the length of an electric Ethernet cable connected to a RJ-45 TPE bushing does not exceed 100 m.
- Make sure the TPE bushing of the system is connected only to safety extra low voltage circuits (SELV circuits).
- If in doubt, ask your system administrator.

For more information, see the documentation of the respective card.

Laser

Personal Injury
If a label with the words CLASS 1 LASER PRODUCT is affixed to the back of your system, the unit is equipped with a laser device. These devices contain a laser diode that produces invisible laser radiation harmful to the eyes.
Performing adjustments or procedures other than those specified in this manual may result in hazardous radiation exposure. Do not look into the optical lens at any time.

Environment

Environmental Damage
Improperly disposing of used products may harm the environment.
Always dispose of used products according to your country's legislation and manufacturer's instructions.

Downloaded from Arrow.com.

Sicherheitshinweise

Dieses Kapitel enthält Hinweise, die potentiell gefährlichen Prozeduren innerhalb dieses Handbuchs vorrangestellt sind. Beachten Sie unbedingt in allen Phasen des Betriebs, der Wartung und der Reparatur des Systems die Anweisungen, die diesen Hinweisen enthalten sind. Sie sollten außerdem alle anderen Vorsichtsmaßnahmen treffen, die für den Betrieb des Systems innerhalb Ihrer Betriebsumgebung notwendig sind. Wenn Sie diese Vorsichtsmaßnahmen oder Sicherheitshinweise, die an anderer Stelle diese Handbuchs enthalten sind, nicht beachten, kann das Verletzungen oder Schäden am System zur Folge haben.

Artesyn ist darauf bedacht, alle notwendigen Informationen zum Einbau und zum Umgang mit dem System in diesem Handbuch bereit zu stellen. Da es sich jedoch bei dem System um ein komplexes Produkt mit vielfältigen Einsatzmöglichkeiten handelt, können wir die Vollständigkeit der im Handbuch enthaltenen Informationen nicht garantieren. Falls Sie weitere Informationen benötigen sollten, wenden Sie sich bitte an die für Sie zuständige Geschäftsstelle von Artesyn.

Das System erfüllt die für die Industrie geforderten Sicherheitsvorschriften und darf ausschließlich für Anwendungen in der Telekommunikationsindustrie, im Zusammenhang mit Industriesteuerungen und in der Entwicklung verwendet werden. Es darf nicht in sicherheitskritischen Anwendungen, lebenserhaltenden Geräten oder in Flugzeugen verwendet werden.

Einbau, Wartung und Betrieb dürfen nur von durch Artesyn ausgebildetem oder im Bereich Elektronik oder Elektrotechnik qualifiziertem Personal durchgeführt werden. Die in diesem Handbuch enthaltenen Informationen dienen ausschließlich dazu, das Wissen von Fachpersonal zu ergänzen, können dieses jedoch nicht ersetzen.

Halten Sie sich von stromführenden Leitungen innerhalb des Systems fern. Entfernen Sie auf keinen Fall die Systemabdeckung. Nur werksseitig zugelassenes Wartungspersonal oder anderweitig qualifiziertes Wartungspersonal darf die Systemabdeckung entfernen, um Systemkomponenten zu ersetzen oder andere Anpassungen vorzunehmen.

Installieren Sie keine Ersatzteile oder führen Sie keine unerlaubten Veränderungen am System durch, sonst verfällt die Garantie. Wenden Sie sich für Wartung oder Reparatur bitte an die für Sie zuständige Geschäftsstelle von Artesyn. So stellen Sie sicher, dass alle sicherheitsrelevanten Aspekte beachtet werden.

Downloaded from Arrow.com.

EMV

Das Produkt wurde getestet und erfüllt die für digitale Geräte der Klasse A gültigen Grenzwerte gemäß den FCC-Richtlinien Abschnitt 15 bzw. EN 55022 Klasse A. Diese Grenzwerte sollen einen angemessenen Schutz vor Störstrahlung beim Betrieb des Produkts in Geschäfts-, Gewerbe- sowie Industriebereichen gewährleisten.

Das Produkt arbeitet im Hochfrequenzbereich und erzeugt Störstrahlung. Bei unsachgemäßem Einbau und anderem als in diesem Handbuch beschriebenen Betrieb können Störungen im Hochfrequenzbereich auftreten. Freie Steckplätze müssen mit Platzhalter-Karten belegt werden, um sicherzustellen, dass die EMV-Richtlinien erfüllt werden.

Benutzen Sie zum Anschließen von Peripheriegeräten ausschließlich abgeschirmte Kabel. So stellen Sie sicher, dass ausreichend Schutz vor Störstrahlung vorhanden ist. Die PCIE Karten müssen mit der Frontblende installiert und alle freien Steckplätze müssen mit Blindblenden abgedeckt sein.

Erdung
Wenn das Produkt nicht richtig geerdet ist, kann es es durch elektrostatische Entladungen beschädigt werden.
Stellen Sie sicher, dass alle Systemteile die EMV-Dichtung berühren. Die Dichtungen befinden sich sowohl am System als auch an den einzelnen Modulen.
Am System befinden sich auch ESD-Kontakte. Stellen Sie sicher, dass jede Person, die mit dem System arbeitet, mit ESD-Schutz, zum Beispiel ESD-Bändern, arbeitet.

Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.

Das Produkt ist für den Einsatz in Netzwerken mit gemeinsamem Potentialausgleich oder mit isoliertem Potentialausgleich geeignet.

System Installation

Beschädigung des Systems
Bevor Sie das System installieren, überprüfen Sie, ob die im Handbuch beschriebenen Anforderungen erfüllt werden.

Downloaded from Arrow.com.

Beachten Sie folgende allgemeinen Sicherheitshinweise vor der Installation und Verkabelung des Systems:

- Überstrom-Schutzeinrichtung: Eine leicht zugängliche Trennvorrichtung muss in der Gebäudeverkabelung eingebaut sein. Einen angemessenen Wert für den Leitungsquerschnitt können Sie der NEC (National Electrical Code) Tabelle 310.16 oder anderen nationalen Regelwerken entnehmen.
- Der Erdungsleiter ist abhängig von der Spannungsverteilungstopologie innerhalb Ihrer Anlage. Stellen Sie sicher, dass Sie einen angemessenen Erdungsleiter gemäß der Auslegung des Zugangsleitungsschutzes verwenden.
- Bauen Sie das System sicher ein. Stellen Sie sicher, dass Kabel und Leitungen nicht im Weg sind.
- Stellen Sie sicher, dass der Systemaufbau anwenderfreundlich ist.

Beschädigung des Systems
Verschmutzungen können das System beschädigen.
Betreiben Sie das System an einem erschütterungsfreien Ort, an dem weder Staub, Rauch noch elektrostatische Entladungen auftreten. Stellen Sie außerdem sicher, dass die klimatischen Bedingungen, die in diesem Handbuch spezifiziert sind, eingehalten werden und genug Raum für die Luftzirkulation vorhanden ist.

Verletzungsgefahr und Beschädigung des Systems (AC)
Das System wird durch die Netzspannung (100V bis 240VAC) versorgt. Diese Spannung kann gefährlich sein. Treffen sie entsprechende Vorsichtsmaßnahmen, wenn sie an der Verkabelung des Systems arbeiten.

Verletzungsgefahr und Beschädigung des Systems (DC)
Das System ist an eine TNV-2-Spannungsquelle angeschlossen. Diese Spannung kann gefährlich sein.
Stellen Sie sicher, dass die externe Spannungsversorgung den entsprechenden Sicherheitsstandards entspricht.
Stellen Sie sicher, dass die TNV-2-Spannungsversorgung von gefährlicheren Spannungsquellen (Hauptstromversorgung) durch doppelte oder verstärkte Isolierung getrennt ist.

Downloaded from Arrow.com.

Verletzungsgefahr und Beschädigung des Systems
Wenn die Gewichte im Schaltschrank ungleich verteilt sind, kann der Schaltschrank umkippen und dadurch die Einrichtungen beschädigen oder Personen verletzen.
Bauen Sie das System deshalb ganz unten im Schrank ein, wenn es das einzige System im Schrank ist. Wenn mehrere Systeme in einen Schrank eingebaut werden sollen, platzieren Sie das schwerste System ganz unten und die leichteren weiter oben. Falls der Schaltschrank mit Kippsicherungen ausgestattet ist, stellen Sie sicher, dass diese auch installiert und ausgefahren sind, um einen sicheren Stand des Schranks zu gewährleisten. Beginnen Sie erst danach mit dem Einbau oder der Wartung des Systems.

Verletzungsgefahr oder Beschädigung des Systems
Das System kann beim Herausziehen herunterfallen und Verletzungen verursachen.
Ziehen Sie das System vorsichtig heraus, damit es nicht herunterfällt.

Verletzungsgefahr
Das System ist schwer, und eine unangemessene Handhabung kann zu Zerrungen oder Rückenschäden führen. Heben Sie deshalb das System nur zu zweit oder benutzen Sie zusätzliche Hilfsmittel. Verwenden Sie zum Heben des Systems nicht die Griffe der Netzteile oder Lüfter.

Beschädigung des Systems
Während des Transportes und Zusammenbaus des Systems können sich Teile, wie zum Beispiel Schrauben, Stecker oder Lüfter, lösen oder beschädigt werden.
Nehmen Sie das System nicht in Betrieb, wenn Teile beschädigt sind. Dies könnte zu Beschädigungen an anderen Teilen führen.

Verletzungsgefahr
Hoher Ableitstrom kann gefährlich sein und Verletzungen verursachen.

Downloaded from Arrow.com.

Stellen Sie fest, wo sich der Aufkleber mit dem Gefahrenzeichen und die zugehörigen Schuzleiter befinden (die Position kann sich bei verschiedenen Systemen unterscheiden). Stellen Sie vor Anschluss des Systems an den Versorgungsstromkreis unbedingt eine Erdungsverbindung her.



Beschädigung des Systems
Falsche Jumper-Einstellungen können dazu führen, dass das System nicht mehr funktioniert. Ändern Sie deshalb nie die Einstellungen der Jumper.

Installation von Einsteckkarten

Produktschaden
Berühren Sie das Karte oder elektrische Komponenten ohne ausreichenden ESD-Schutz, kann dies zu einer Beschädigung des Karten führen.
Bevor Sie Karten berühren, vergewissern Sie sich, dass Sie in einem ESD-geschützten Bereich arbeiten, oder tragen Sie ein ESD-Handgelenkband oder ESD-Schuhe. Fassen Sie Karten nur an der Seite an und berühren Sie keine elektronischen Komponenten.

Beschädigung des Karten oder Systems
Wird ein PCIE-Karte in den falschen Steckplatz im System gesteckt, können sowohl das Karte als auch das System beschädigt werden. Installieren Sie Karten deshalb ausschließlich in dafür vorgesehene Steckplätze.

Datenverlust
Das MaxCore System bietet keine Unterstützung für das Wechseln von PCIe Karten in laufendem Betrieb. Stellen Sie sicher, daß die Stromversorgung der PCIe Steckplätze abgeschalten ist, bevor sie das System öffnen und PCIe Karten entfernt bzw. hinzugefügt werden.

Downloaded from Arrow.com.

Fehlfunktion
Unsachgemäßer Ein- und Ausbau von PCIE-Karten kann zu einer Fehlfunktion des PCIE-Karten führen.
Vergewissern Sie sich, dass das Karte über alle Stecker an die Backplane angeschlossen und die Stromversorgung gewährleistet ist.

Betrieb

Überhitzung des Systems
Lüftungsschlitze
Unzureichende Lüftung kann Schäden an PCIE-Karten und am System verursachen und den Verlust der Garantie zur Folge haben.
Um eine ausreichende Lüftung zu gewährleisten, stellen Sie sicher, dass das System während des Betriebs stets waagerecht steht. Halten Sie die Lüftungsschlitze an der Vorder- und Rückseite des Systems frei. Halten Sie die Frischluftzufuhröffnung an der Vorderseite des Systems völlig frei und stellen Sie sicher, dass sich die Frischluft nicht mit der Abluft von anderen Systemen mischt. Um eine ungestörte Luftzirkulation zu gewährleisten, stellen Sie sicher, dass alle Steckplätze mit PCIE-Karten oder Platzhaltern belegt sind.

Beschädigung des Systems
Durch hohe Luftfeuchtigkeit können Kurzschlüsse entstehen.
Betreiben Sie das System nur innerhalb der angegebenen Grenzwerte für die relative Luftfeuchtigkeit und Temperatur. Stellen Sie vor dem Einschalten des Stroms sicher, dass sich auf dem System und auf den PCIE-Karten kein Kondensat befindet und starten Sie das System nicht unter 0ºC.

Stromschlaggefahr
Das System besitzt drei Anschlüsse für die Netzspannung (100V bis 240VAC) / drei Anschlüsse für -48V bis -60VDC. Alle Anschlüsse müssen vom System entfernt werden, um das System spannungsfrei zu schalten.
Um eine Verletzungsgefahr zu minimieren, entfernen Sie die Anschlüsse, wenn Sie das System ausschalten.

Downloaded from Arrow.com.

Beschädigung des Systems
Luftfilter
Verunreinigungen in der Luft können den Luftfilter verschmutzen und so die Luftzufuhr des Systems beeinträchtigen. Das kann zur Überhitzung des Systems und zu Schäden an Systemteilen führen.
Um einen reibungslosen Luftstrom durch das System zu gewährleisten, sollten Sie die Luftfilter spätestens alle sechs Monate austauschen. Artesyn empfiehlt, die Filter alle 90 Tage auszutauschen. Je nach Umgebungsbedingen kann dies aber auch früher nötig sein.
Da die Verhältnisse in Vermittlungsstellen sehr unterschiedlich sein können, sollten Sie die Luftfilter nach der Erstinstallation des Systems jede Woche kontrollieren. In einer staubigen Umgebung muss ein Filter gegebenenfalls öfter ausgetauscht werden als in einer sauberen Umgebung. Prüfen Sie die Filter regelmäßig, bis Sie eine Vorstellung davon haben, wie oft die Filter ausgetauscht werden müssen. Erstellen Sie aufgrund Ihrer Beobachtungen einen Plan für den Austausch und protokollieren Sie jeden Austausch des Filters.

Filterrahmen
Wenn Sie einen Rahmen falsch einbauen, kann dies den Rahmen oder das Front Panel beschädigen.
Das Front Panel inklusive Luftfilter wird mittels Führungsstiften und Halteclips am System befestigt. Achten Sie bei der Montage des Frontpanels auf die korrekte Ausrichtung.

Überhitzung des Systems
Wenn Sie die Lüftergeschwindigkeit manuell einstellen, dann überwachen Sie bitte regelmäßig die Temperaturen des Systems, um eine Überhitzung zu vermeiden.

Verletzungen oder Kurzschlüsse
Prüfen Sie immer, ob die System spannungsfrei ist, nachdem sie das Anschlussleitungen vom System getrennt haben, bevor Sie Ihre Arbeit fortsetzen, um Schäden oder Verletzungen zu vermeiden.

Downloaded from Arrow.com.

Systemerweiterung

Systemüberlastung
Verhindern Sie eine Systemüberlastung, indem Sie die gesamte aufgenommene Leistung aller eingebauten Komponenten, also z.B. der installierten PCIE-Karten und Laufwerke (siehe die technischen Daten der entsprechenden Komponente) überprüfen. Bei Ihrem System darf die Gesamtleistung die im Abschnitt Power Requirements definierten Werte nicht überschreiten.

Verlust der Sicherheitszulassung
Verwendung zusätzlicher Module
Wenn Sie zusätzliche Module und Karten verwenden, ist es möglich, dass das System nicht mehr den gültigen Sicherheits- und EMV-Normen entspricht. Der Systemintegrator muss die Einhaltung der gültigen Normen sicherstellen.

Stromzufuhr

Verletzungsgefahr
Berühren metallische Gegenstände an Händen, Handgelenken oder am Hals die Stromzufuhr, kann dies zu schweren Verletzungen durch Stromschlag oder Verbrennungen führen. Tragen Sie bei der Arbeit mit dem System keine metallischen Gegenstände an Ihren Händen oder Armen und lassen sie keine metallischen Gegenstände um Ihren Hals hängen. Seien Sie extrem vorsichtig mit elektrisch leitenden Werkzeugen und Gegenständen in der Nähe der PSUs.

Kurzschluss und Gefahr durch Stromschlag
Um einen elektrischen Schlag zu vermeiden, überzeugen Sie sich, dass vor dem Berühren der stromführenden Zuleitungen die Stromzufuhr unterbrochen ist und während der Arbeit unterbrochen bleibt. Vermeiden Sie Kurzschlüsse, indem Sie sehr vorsichtig mit dem Werkzeug umgehen.

Beschädigung des Systems
Falscher Anschluss von Stromkabeln kann das System beschädigen..
Achten Sie darauf, dass Sie das Stromkabel mit der richtigen Polarität anschließen..

Downloaded from Arrow.com.

AC PSUs

Verletzungsgefahr
Das Berühren von heißen Netzteilen kann zu Verletzungen führen.
Lassen Sie die Netzteile abkühlen, bevor Sie sie mit bloßen Händen herausziehen.

DC PSUs

Verletzungsgefahr
Das Berühren von heißen Netzteilen kann zu Verletzungen führen.
Lassen Sie die Netzteile abkühlen, bevor Sie sie mit bloßen Händen herausziehen.

Beschädigung des Systems
Wenn Sie ein Netzteil aus dem System ausbauen oder in das System installieren, während die Versorgungsleitung angeschlossen und die Spannungsversorgung angeschalten ist, kann dies das Netzteil oder Ihr System beschädigen.
Wenn die Versorgungsleitung angeschlossen ist, stellen Sie sicher, dass die Spannungsversorgung an der PDU ausgeschalten ist, bevor Sie ein Netzteil installieren oder ausbauen.

Beschädigung der Netzteile
Der Betrieb der Netzteile, während ein dauerhafter Kurzschluss im System vorliegt, kann die Netzteile beschädigen.
Stellen Sie deshalb sicher, dass kein Kurzschluss im System vorliegt.

Lüftermodule

Beschädigung des Systems
Unzureichende Kühlung kann das System beschädigen.
Das Lüftungssystem ist so ausgelegt, dass ein einzelnes funktionierendes Lüftermodul für ausreichende Lüftung sorgt. Unter ungünstigen Umständen oder bei einer Fehlfunktion der verbleibenden Lüfter reicht die Lüftungsleistung eines einzelnen Lüftermoduls aber möglicherweise nicht aus. Nehmen Sie deshalb den Austausch ohne Verzögerung vor.

Downloaded from Arrow.com.

Beschädigung von Lüftern
Wenn ein Lüfter außer Betrieb ist oder während einer Austauschprozedur aus dem System entfernt wird, veranlasst der System-Manager die übrigen Lüfter dazu, mit höherer Geschwindigkeit zu drehen. Wenn Lüfter über einen längeren Zeitraum mit hoher Geschwindigkeit laufen, kann das ihre Lebenszeit verkürzen und die zulässigen Lärmgrenzwerte übersteigen.
Tauschen Sie das Lüftermodul ohne Verzögerung aus.

Beschädigung des Systems
Wenn Sie das einzige funktionierende Lüftermodul entfernen, kommt es in sehr kurzer Zeit zu einer Überhitzung.
Stellen Sie sicher, dass sich immer mindestens ein funktionierendes Lüftermodul im System befindet.

Verletzungsgefahr
Rotierende Lüfterschaufeln
Sie können verletzt werden, wenn Sie Werkzeuge oder Finger in laufende Lüfter einführen.
Berühren Sie die Lüfterschaufeln nicht, solange sie sich drehen.

Verkabelung/Kabelführung

Verletzungsgefahr
Verändern Sie nie die von Artesyn ausgelieferte Verkabelung des Systems.
Stellen Sie sicher, dass die Verkabelung schon existierenden Kabelführungen folgt und bestehende oder ähnliche Befestigungen verwendet. Überprüfen Sie nach der Erweiterung der Verkabelung, ob das System ordnungsgemäß arbeitet.
Reduzieren Sie die Verletzungsgefahr, indem Sie Kabel so verlegen, dass niemand darüber stolpern kann.

Verletzungsgefahr durch Stromschlag
Durch das Berühren von Kontakten und Kabeln während des Betriebs können Sie einen elektrischen Schlag bekommen.

Downloaded from Arrow.com.

Schließen Sie in jedem Fall aus, dass Personen durch einen elektrischen Schlag verletzt werden können, indem Sie sicherstellen, dass Kontakte und Kabel des Systems während des Betriebs nicht berührt werden können.
Falls Sie Fragen bezüglich der Verkabelung haben, wenden Sie sich an die für Sie zuständige Geschäftsstelle von Artesyn.

Beschädigung der Kabel
Werden Kabel geknickt, kann das Kabel beschädigt werden und der Datentransfer nicht mehr stattfinden. Stellen Sie sicher, dass Kabel nicht geknickt werden.

RJ-45 Stecker

Beschädigung des Systems
Bei den RJ-45 Steckern, die sich am I/O Modul des Systems oder auf den PCIE-Karten befinden, handelt es sich entweder um Twisted-Pair-Ethernet (TPE) oder um E1/T1/J1-Stecker. Beachten Sie, dass ein versehentliches Anschließen einer E1/T1/J1 Leitung an einen TPE-Stecker Ihr System zerstören kann.

- Kennzeichnen Sie deshalb TPE-Anschlüsse in der Nähe Ihres Arbeitsplatzes deutlich als Netzwerkanschlüsse.
- Stellen Sie sicher, dass die Länge eines Ethernet Kabels, das mit Ihrem System verbundenen ist, 100 m nicht überschreitet.
- Das System darf über die TPE Stecker nur mit einem Sicherheits-Kleinspannungs-Stromkreis (SELV) verbunden werden.
- Bei Fragen wenden Sie sich an Ihren Systemverwalter.

Weitere Informationen finden Sie in der Dokumentation des jeweiligen PCIE-Karten.

Downloaded from Arrow.com.

Laser

Verletzungsgefahr
Wenn sich an der Rückseite Ihres Systems ein Aufkleber mit der Aufschrift CLASS 1 LASER PRODUCT befindet, beeinhaltet das System ein Bauteil mit einem Laser. Solche Bauteile enthalten Laserdioden, die unsichtbare und für die Augen schädliche Laserstrahlen abgeben. Falls Sie sich nicht an die Anweisung in diesem Handbuch halten, kann dies zu gefährlichen Strahlungsbelastungen führen. Schauen Sie niemals direkt in den Laserstrahl.

Umweltschutz

Umweltschäden
Unsachgemäße Entsorgung von Produkten kann zu Umweltbelastungen führen.
Entsorgen Sie gebrauchte Produkte stets gemäß der in Ihrem Land gültigen Gesetzgebung und den Empfehlungen des Herstellers.

Downloaded from Arrow.com.

Product Documentation Overview

MaxCore™ MC3000 is a platform for designing a highly scalable rack-mount appliance. The overall objective of this platform is to enable a wide range of solution providers to create their own competitive appliances and achieve the best time-to-market advantages. This implies the ability to integrate building blocks from a huge portfolio of existing hardware and software components that are available in the market or from within their own design centers. This also implies an abstraction, which allows a primarily software focused solution design team to operate within their comfort zone.

MaxCore is a Rack Mount Server (RMS) with PCIe card slots. MaxCore differs from that of classical enterprise server in the sheer number of PCIe card slots available and its ability to implement many network connected servers within the same enclosure. These servers are independent CPUs that represent a root for a PCI device tree. A significantly differentiating feature of MaxCore is that many CPUs can now share a single PCIe card, for example, a network I/O card. In addition, MaxCore provides PCIe based network interconnects between CPUs.

The following section provides the list of documents to understand MaxCore, its components, features, and operation. These documents guide you to start, operate, maintain, configure, and manage a MaxCore system. Based on their purpose and significance, these documents can be categorized into the following types:

- **MaxCore™ MC3000 Platform**: The manuals under this category explain MaxCore and its hardware components' description, installation and removal procedures, functions, safety notices, and OS related information.
  - **MaxCore™ MC3000 Platform Quick Start Guide**: Helps you to jump start with a new MaxCore system from the factory. This document helps you to become familiar with the product and gives you the perspective to decide what is most important for you to know and how to start using MaxCore. A printed copy of this manual is shipped along with the MaxCore system.
  - **MaxCore™ MC3000 Platform Safety Notes Summary**: Contains safety precautions you may need to follow while installing or servicing the system or accessories. If not followed properly, there are chances of occurring personal injury or property damage. Ignoring these instructions can void the system warranty. A printed copy of this manual is shipped along with the MaxCore system.
  - **MaxCore™ MC3000 Platform Installation and Use**: Describes MaxCore as a classical enterprise server with a single CPU and many empty slots for PCIe cards. This manual covers the hardware, the system management access entry over the Board Management Controller (BMC), the bring up of the pre-installed Linux, and the installation of a new Operating System.

Downloaded from Arrow.com.

  - **MaxCore™ MC3000 Rail Kit Installation Quick Start Guide**: Describes the rail kit components and MaxCore rack mount slides installation procedure. A printed copy of this manual is shipped along with the MaxCore system.
  - **MaxCore™ MC3000 Platform Software Installation and Use**: Provides information on how to install MaxCore MC3000 Platform software on Artesyn MaxCore PCIE cards.

- **SSF for MaxCore™ MC3000 Platform**: The manuals under this category explain how System Services Framework (SSF) is used to manage and configure the MaxCore system and its components. SSF comes pre-installed from the factory. It is hosted by the main CPU (shelfHost) of MaxCore. SSF covers most of the BMC functionality and is recommended as the primary interface for MaxCore management, except the functions which can only be provided by the always powered BMC (remote power button, serial console over LAN). Using SSF, you can change MaxCore from the factory configured single-CPU (Base) mode to a multi-CPU (Express Fabric) mode.
  - **SSF for MaxCore™ MC3000 Platform XML Guide**: Provides a detailed description on how to facilitate system level configuration and management access of hardware and software components through SSF via XML interface.
  - **SSF for MaxCore™ MC3000 Platform CLI Guide**: Provides a detailed description on usage of Command Line Interface (CLI) to work with SSF.
  - **SSF for MaxCore™ MC3000 GUI Help**: Provides a detailed description on usage of graphical user interface to work with SSF.

For complete list of documents, refer to the section *Artesyn Embedded Technologies - Embedded Computing Documentation* on page 241.

Downloaded from Arrow.com.

This chapter provides information on MaxCore system views, system management, and a brief description about the hardware components available in a MaxCore system.

2.1 System Views and Components

MaxCore system is a 3U box of height 132 mm with a depth of 508 mm, which fits into 19” racks. The chassis provides front to rear cooling via redundant fan modules. Either AC or -48 V DC power module options are available, which are connected to the rear of the chassis. Both cooling and power FRUs are fault-tolerant and can be serviced while the system is in operation.

Integrated chassis mounting flanges are attached at each side of the system to front mount the shelf into a rack. You can install the system in a standard 19" ANSI rack using the integrated chassis mounting flanges. Furthermore, extension brackets for 23" ANSI and 600 mm ETSI racks are available.

At least one slot always hosts SharpServer, an Artesyn CPU card. Each of the other slots can either host another SharpServer card or a full-size Commercial-off-the-Shelf (COTS) based PCIe card. SharpServer is MaxCore-specific, as there is no public standard for the so-called root-complex (the only CPU in a PCI device tree) in a PCIe card slot. SharpServer itself hosts two fully independent Xeon-D CPU subsystems.

MaxCore offers 15 PCIe card slots that provide the following capabilities:

- 11 slots are PCIe Gen3.0 x8 capable for a net bandwidth of 50 Gbps through the card.
- Four (4) slots are PCIe Gen3.0 x16 capable for a net bandwidth of 100 Gbps.

Downloaded from Arrow.com.

Figure 2-1 and Figure 2-2 show front and rear views of the MaxCore system.

Figure 2-1 MaxCore Front View

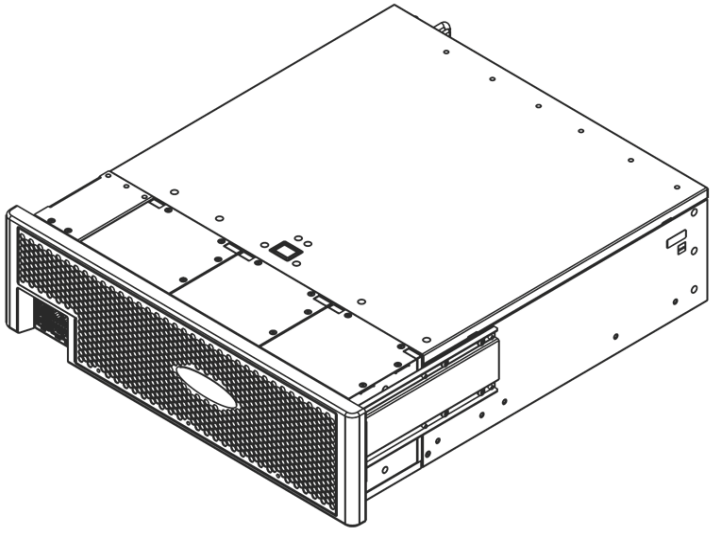
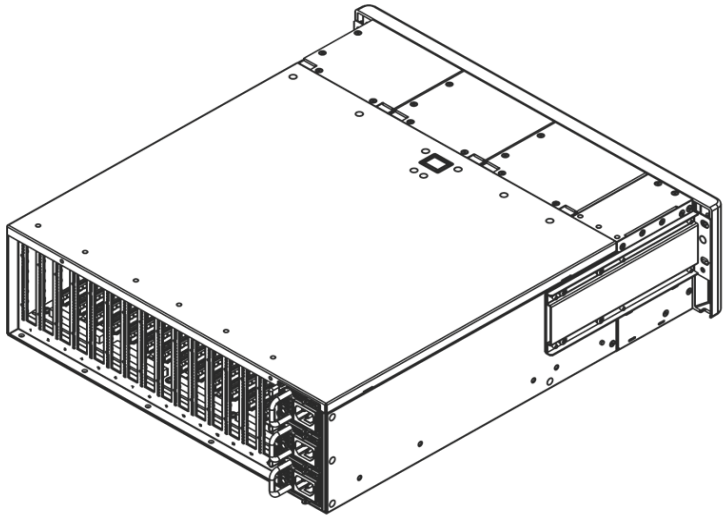


Figure 2-2 MaxCore Rear View



Downloaded from Arrow.com.

2.1.1 PCIe Card Slots

The MC3000 system provides 15 PCIe card slots, oriented vertically in the system. They are accessible from the top of the system after removing the top lid.

Four (4)out of these 15 slots support a PCIe x16 connection and the remaining slots support a PCIe x8 connection.

2.1.2 Processor Subsystem

The MC3000 system comes with an Artesyn's SharpServer™ PCIE-7410 card installed in slot #1.

The PCIE-7410 card contains following components:

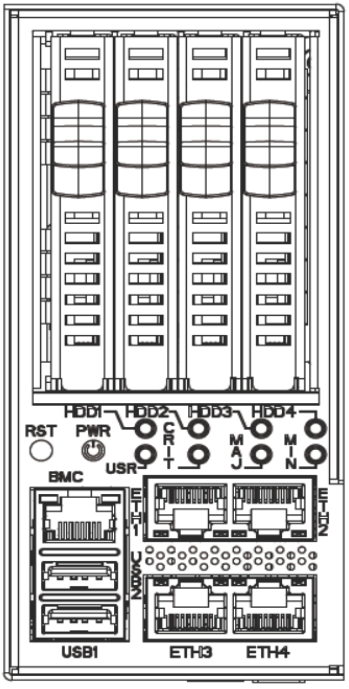
- Intel® Xeon® Processor D - SoC processor.
- 32 GB DDR4 memory (in 4 SODIMM sockets).
- Two (2) SATA 3 ports to the systems HDD drive bays.
- Onboard microSD card as optional local boot media.
- USB 2.0 port at the PCIe card's faceplate (accessible at the rear of the system).
- USB 2.0 port at the system's IO panel.
- USB 2.0 port to system's BMC port for remote media access.
- Processor COM port via USB at the PCIe card's faceplate.
- Processor COM port via SOL, accessible through the system's BMC.

Downloaded from Arrow.com.

2.1.3 IO Panel

The IO panel is located at the front of the system.

Figure 2-3 IO Panel



The IO panel provides the following interfaces and features:

- Four (4) HDD drive bays (accessible after removal of the snap-in system front bezel)
- One (1) 1 Gigabit Ethernet (RJ45) port from the BMC
- Two (1) 1 Gigabit/10 Gigabit Ethernet (RJ45) ports from the CPU via an Intel 82599 Niantic controller (ETH3, ETH4)
- Two (2) 1 Gigabit Ethernet (RJ45) uplink ports from a 1G Ethernet switch (ETH1, ETH2) connecting all installed CPUs in the system
- Two (2) USB 2.0 ports from the CPU

Downloaded from Arrow.com.

- Power button
- Reset button (no function assigned, reserved)
- HDD indicators
- User indicator
- Alarm indicators (CRIT, MAJ, MIN)

The assignment of HDD and USB ports to specific CPUs installed in slot 1 and slot 15 can be configured via Artesyn's SSF.

2.1.3.1 Disk Drive Bays

The system provides four (4) disk drive bays for 2.5" SATA disk drives. The SATA3 interface standard is supported. Disks in these drive bays are accessible from the MC3000 slots 1 and 15 only.

2.1.4 AC and DC Power Supply Modules

The MC3000 supports up to three redundant hot-swappable AC or DC power supplies.

The power supplies can either be operated in a non-redundant mode providing up to 3300 W total electrical power or in a redundant 2+1 mode providing up to 2200 W total electrical power.

2.1.5 Fan Modules

The system provides fault-tolerant cooling by using three hot-swappable fan modules accessible from the front of the system after removing the system's front bezel. Each fan module contains two fans, which are speed-controlled by BMC.

2.1.6 Air Filter and Front Bezel

The front side of the MC3000 system is covered by a snap-in front bezel.The air filter is installed inside the front bezel. It ensures that the system operates efficiently and therefore regular maintenance or replacement of the air filter is required.

A Green LED indicates proper operation of the fan, a Red LED indicates the fan is off or faulty.

Downloaded from Arrow.com.

2.2 System Management

The MC3000 system is managed through a BMC running AMI's MegaRAC software.

Using the BMC, you can perform the following tasks:

- Power-Up and Power-Down control of the system
- Thermal Management / Fan Speed Control
- CPLD Firmware Update
- System Configuration Management

The BMC is accessible via its web interface through the BMC 1GE interface on the IO panel. For more information about BMC, refer to *Remote Management via Board Management Controller* on page 117.

Downloaded from Arrow.com.

2.3 Standard Compliances

The product has been designed to meet the following standards.

Table 2-1 Standard Compliances

Standard	Description
UL 60950-1 EN 60950-1 IEC 60950-1 CAN/CSA C22.2 No 60950-1	Safety requirements (legal)
AS/NZS CISPR 22 CISPR 22 CISPR 24 EN 55022 EN 55024 EN 300 386[1] FCC Part 15 Industry Canada ICES-003 NEBS Standard GR-1089 CORE VCCI Japan	EMC requirements (legal) on system level (predefined Artesyn system)
ETSI ETS 300 753 NEBS Standard GR-63-CORE ETSI EN 300 019 series	Environmental requirements
ETSI EN 300 132-2	Power requirements

1. When using the MC3000 outside telecommunication centers, the integrator must take additional measures to comply with EN 300386 requirements for EN 61000-4-11 (Voltage Dips and Interruptions).

Downloaded from Arrow.com.

The products listed in the ordering information for spare parts and accessory kits are designed to meet the Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS), DIRECTIVE 2011/65/EU.

The system is compliant to NEBS and ETSI acoustic noise emission standards, if the system is equipped with Artesyn cards and with respectively designed and configured third party cards. In a system thus configured, the fans will settle at approximately 10%-20% speed at an ambient temperature of 23 °C (+/- 2° C) (73.4 °F +/- 3.6 °F) under normal operating conditions.

To fulfill the requirements of Telcordia GR-1089, R4-14, use Shielded Twisted Pair (STP) cables grounded at both ends to connect to the Ethernet ports.

For more information, refer to *Telcordia GR-1089-CORE, section 9.8.2, requirement R9-14*.



To satisfy the requirements for marking electrical and electronic equipment in accordance with article 11 (2) of Directive 2002/96/EC, Waste from Electrical and Electronic Equipment (WEEE), Artesyn includes a crossed-out bin symbol on all standard and non-custom chassis product. This marking fulfills the requirement set out by WEEE that a producer of an electrical or electronic appliance that bears their trade name and is put on the European Union market after 13 August 2005, places a clearly identifiable mark on the equipment and that this mark

Downloaded from Arrow.com.

signifies that equipment is to be reprocessed or recycled using authorized recyclers and processes. This minimizes the disposal of unsorted municipal waste, achieves a high level of separate collection of WEEE, and ensures the environmentally sound disposal of electrical and electronic equipment placed on the market after 13 August 2005.

To dispose of equipment marked with the WEEE symbol, Artesyn has contracted with certified companies that can reprocess this equipment per European Union requirements. Please visit the Artesyn web site or contact your Artesyn representative to find out who to contact and how to dispose of the equipment.

2.4 Ordering Information

As of the printing date of this manual, the system models and spare parts listed below are supported.

Table 2-2 Ordering Information

Part Number	Description
Platform Core Products	
MC3000-00R	MaxCore Chassis
MC3000-01R-2	MaxCore with1X Dual CPU Micro Server Cards
MC3000-FIO-40G	Front I/O Panel, 40 GB for MaxCore
Board Variants	
PCIE-7410-2	Micro Server card for 3U RMS - 2X CPU
PCIE-7207-4	PCIe card, 4X Intel Core I7, Video Transcode
Accessory Kits	
MC3000-SSD-1TB-SATA	1TB MLC 2.5 inch SSD
MC3000-SSD-512G-SATA	512 GB MLC 2.5 inch SSD
MC3000-MEM-64GBSD	64 GB Secure Digital Memory Card for MC3000
MC3000-I/O-USB-CBL	Auxiliary I/O, USB A-TO-MICRO-USB
MC3000-NIC-X520S	Ethernet Network Adapter X520-SR2
MC3000-RAIL	Rack mount slides for MC3000
MC3000-MEM-8GBSODIMM	8 GB Small outline memory module for MC3000

Downloaded from Arrow.com.

Table 2-2 Ordering Information (continued)

Part Number	Description
MC3000-SLT-FLR	Slot blocker panel for MaxCore 3000
MC3000-PSU	AC Power Supply for MC3000
MC3000-DC-PSU	DC Power Supply for MC3000
QSFPP-40G-SR4-MODULE	40G QSFP+ Module - 40GBASE-SR4 - 850NM - for multimode fiber - MTP (MPO) connector
MC3000-FAN	Fan module for MC3000
MC3000-HDD-CARR	HDD carrier for MC3000
MC3000-ACC-CBL	Auxiliary 12 V Power Cable for MC3000
MC3000-ACC-Y-CBL	Auxiliary 12 V Power-Y-Cable for MC3000
Power Cords	
AC-PC-20A-PIGTAIL	AC power cord, right angle, 20 amps, 250 volts, pigtail
AC-PC-13A-UK	AC power cord, 13 amps, 250 volts, UK connector
AC-PC-15A-AUS-ZEL	AC power cord, 15 amps, 250 volts, Australia & New Zealand connector
AC-PC-16A-EU	AC power cord, 16 amps, 250 volts, EU connector
AC-PC-20A-US-250V	AC power cord, 20 amps, 250 volts, US & Canada connector

Downloaded from Arrow.com.

This chapter provides information on unpacking the system procedure, safety precautions, and requirements for the product. The environmental and power requirements, mounting options, cooling considerations, acoustic noise control, and dimensions and weight of the system are explained in this chapter.

3.1 Site Planning Considerations

This section provides information to prepare the site and the system for installation.

3.1.1 Unpacking the System

Carefully inspect the system and all the components delivered together with it.

NOTICE

Damage of Circuits
Electrostatic discharge and incorrect installation and removal of the product can damage circuits or shorten their life.
Before touching the product make sure that your are working in an ESD-safe environment or wear an ESD wrist strap or ESD shoes. Hold the product by its edges and do not touch any components or circuits.

Shipment Inspection

To inspect the shipment, perform the following steps:

1. Verify that you have received all items of your shipment.
   Compare the shipment thoroughly with the delivery note.
2. Visually inspect the shelf to ensure that all of the connector pins are straight, shrouds are properly seated, screws are tight, and so on.
3. Check the rails for proper alignment.
4. Check that the air filters are properly installed.
5. Check that the cable connections are secure and properly fitted.

Downloaded from Arrow.com.

6. Check the EMI gaskets for damage.
7. If any damage or discrepancies are observed with the items listed above, request an RMA for product return at RMASupport.ec@Artesyn.com.
8. Tighten loose screws before proceeding.
9. Remove the desiccant bags delivered together with the system and dispose of them according to your country's legislation.



The MaxCore is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, please contact our customer's service immediately.

3.1.2 Site and Installation Planning

The following are the basic site planning and installation requirements.

- Adequate power should be available for the MC3000 system.
- For AC, the system should be positioned in a way that 100 VAC to 240 VAC power source is easy to reach.
- For DC, the system should be positioned in a way that -48 VDC to -60 VDC power source is easy to reach.
- Sufficient space should be available in racks to install the system.
- Suitable equipment should be available to lift the system into the rack.
- Enough space should be available to run a system console terminal (only if you want to use a local terminal). The cable should be long enough to reach the system.
- Ensure that the inlet and outlet of the fans is not blocked.
- Should be installed in a restricted access location.
- Should have access to trained personnel only.

Downloaded from Arrow.com.

3.2 Precautions



⚠ WARNING

- **To reduce the risk of personal injury, fire, or damage to the equipment, do not overload the AC supply circuit that provides power to the chassis.**
- **The board must be powered and connected only to a controlled voltage source.**
- **To avoid shock, make sure that the chassis power cables are connected to a properly wired and grounded receptacles.**

NOTICE

Electrostatic Discharge
Do not touch the circuit board with bare hands.
The static electricity of the human body may damage the ElectroStatic Sensitive Devices (ESSDs) on the circuit board.
Make sure that you wear an ElectroStatic Discharge (ESD) preventive wrist strap or antistatic glove to prevent the static electricity from hurting you or damaging the device.
Keep your personal objects such as your clothes away from the system. To prevent the static electricity from damaging the device, it is recommended to wear antistatic clothes.

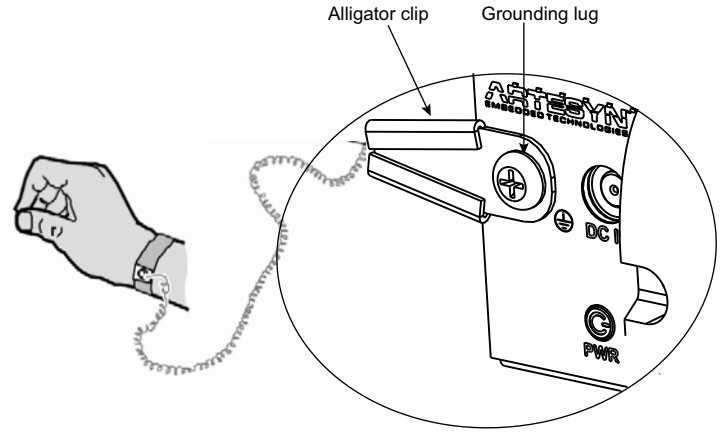
Pin Damage
If the board is not fully aligned with the interface in the backplane, too much force may twist the pins on the card or backplane.
Do not exert too much force when you insert the card.

Downloaded from Arrow.com.

3.2.1 ESD Prevention

Static electricity may hurt you or damage the device. To minimize the damage, pay attention to the following points:

- Before touching the card or electronic components, make sure that you are working in an ESD safe environment.
- Before you operate the device, wear the ESD-preventive wrist strap. Both terminals of the ESD preventive wrist strap must contact well. One terminal touches your bare skin and attach the other terminal with alligator clip to the grounding lug at IO panel of the system



- Avoid moving as much as possible. Movement gathers static electricity around you.
- Do not touch the solder point, pin, or bare circuit.
- Do not leave the device in the place where others can operate it.
- Install the device at once after you take it out of the anti-static package. If you need to lay down the device, place it back in the anti-static package. Do not lay the device on the shelf or cabinet.
- Monitor the temperature and humidity of the equipment room. Warm air decreases the humidity but increases the static electricity in the room.

Downloaded from Arrow.com.

NOTICE

Damage of Circuits
Electrostatic discharge and incorrect module installation and removal can damage circuits or shorten their life. Before touching the module or electronic components, make sure that you are working in an ESD safe environment.

3.3 Requirements

Before and during system installation and operation, you always have to ensure that the requirements listed in the following sections are met.

3.3.1 Environmental Requirements

To ensure proper function of the system, make sure that the environment in which the system is to be used fulfills the environmental requirements.

The environmental values must be tested and proven in the planned system configuration, that is, the delivered system and other third-party products you want to integrate.



- **Operating temperatures refer to the temperature of the air circulating at the air intake of the system and not to component temperatures.**
- **Some of the climatic values may exceed the specification of some system components (for example, hard disks). As Artesyn cannot guarantee the functionality of third party products that are handled or operated out of their specifications, the environmental conditions may be limited to the specifications of these components.**

Downloaded from Arrow.com.

The following table lists the environmental requirements.

Table 3-1 Environmental Conditions

Feature	Operating	Non-Operating (packed state)
Temperature	0 °C (32 °F) to +35 °C (95 °F)	-40 °C (-40 °F) to +70 °C (158 °F)
Temperature change	+/-0.5 °C/min according to NEBS standard GR-63-CORE	+/-0.5 °C/min
Relative humidity	5% to 90% non-condensing according to Artesyn-internal environmental requirements	5% to 95% non-condensing according to Artesyn-internal environmental requirements
Vibration (tested in target platform)	0.1 g from 5 to 100 Hz and back to 5 Hz at a rate of 0.1 octave/minute	5-20 Hz at 0.01 g^2/Hz 20-200 Hz at -3.0 dB/octave Random 5-20 Hz at 1m^2/Sec^3 Random 20-200 Hz at -3 dB/octave
Shock	Half-sine, 11 mSec, 30 m/Sec^2	Card level packaging Half-sine, 6 mSec at 180 m/Sec^2
Free fall	-	800 mm (packaged) 10 kg to 25 kg: 75 mm, >25 kg: 50mm (unpacked) per GR-63-CORE fully populated system
Noise	ETSI ETS 300 753 (Oct. 1997) Telecommunication equipment rooms (attended): 7.2 Bel Measurement of "declared A-weight sound power level" All values are applicable to normal operating conditions (~23 °C/73.4 °F) NEBS GR-63-CORE, Issue 3 Telecommunication equipment rooms (attended): 78 dB Measurement of "declared A-weight sound power level" All values are applicable to normal operating conditions (~27 °C/80.6 °F).	-

Downloaded from Arrow.com.

- **The ambient temperature is defined as the air inlet temperature.**
- **The system regulates the fan speed based on the temperature sensors present in the shelf. The fan speed is adjusted to the lowest speed, which still keeps the evaluated temperature readings below or at their respective "upper non-critical threshold". Hence, the fan speed depends on the ambient temperature, card design, temperature threshold settings, and system configuration.**

To guarantee proper card operation, you have to make sure that the temperatures at the locations specified in the following are not exceeded. If not stated otherwise, the temperatures should be measured by placing a sensor exactly at the given locations.

Table 3-2 Critical Temperature Limits

Component	Maximum Temperature
Air inlet (Front)	35 °C (95 °F)
Air outlet (Rear)	70 °C (158 °F) >70 °C (158 °F) and maximum 90 °C (194 °F): the cables must be isolated and must be approved to be used in this temperature range. >70 °C (158 °F) and maximum 90 °C (194 °F): If you operate the system at >70 °C, make sure that the cables are isolated and that the "hot surface" icon is attached. The cables must be approved to be used in this temperature range. 

Downloaded from Arrow.com.

3.3.2 Power Requirements

Make sure that the rated power source of 100 VAC to 240 VAC for AC and -48 VDC to -60 VDC for DC is within the reach of the system. Up to three Power Supply Units (PSUs) can be installed in the system.



⚠ CAUTION

Personal Injury or System Damage

MC3000 AC
The system is supplied by an AC voltage. External wiring shall be compliant to all requirements of National Electric Code (NEC).

MC3000 DC
The system is supplied by a TNV-2 voltage. This voltage is considered hazardous. Make sure that the external power supply meets the relevant safety standards. Ensure that TNV-2 is separated from dangerous voltages (mains) through double or reinforced insulation.

Table 3-3 AC System Power Requirements

Feature	Value (For AC)
Rated voltage and input current	100 VAC to 240 VAC and 12 A Maximum
Operating voltage range	90 VAC to 254 VAC

Table 3-4 DC System Power Requirements

Feature	Value (For DC)
Rated voltage and input current	-48 VDC to -60 VDC, 32 A Maximum US and Canada: -48 VDC, 32 A Maximum
Operating voltage range	-40 VDC to -72 VDC US and Canada: -40 VDC to -60 VDC

Downloaded from Arrow.com.

Table 3-4 DC System Power Requirements (continued)

Feature	Value (For DC)
Maximum power dissipation	The MC3000 system is tested for a total maximum power dissipation of 2200 W in a 2N+1 power supply configuration. In a three PSU configuration, the total power consumption can be up to 3300 W, but the total power dissipation will be limited by the cooling capability of the system (~2600 W).



When installing additional PCIe cards or modules, make sure that the power consumption of all installed modules does not exceed the system's maximum power dissipation.

The current values provided in the Table 3-3 and Table 3-4 are for a single PSU (12 A for AC and 32 A for DC). As we have up to three PSUs in the system, the system is powered by up to 3 x 12 A for AC and 3 x 32 A for DC PSUs respectively.

The following table lists typical power consumption values of the platform elements and may help to estimate the power budget of a specific system configuration.

Table 3-5 Typical Power Consumption Values

Platform or Element Name	Value
MC3000-01R-2 (system with one PCIE-7410-2 included)	520 W
PCIE-7410-2	120 W

Downloaded from Arrow.com.

3.4 Dimensions and Weight

The table below lists the dimensions and weight of the system and its components.

Table 3-6 Dimensions and Weight of System and Components

Component	Dimensions w x h x d (in mm)	Weight in Kg
System including three fan modules, three AC PSUs and Front Bezel (incl. Air Filter)	482 x 133 x 542	19
AC PSU	58 x 42 x 363	1.1
DC PSU	58 x 42 x 363	1.0
Fan Module	123 x 133 x 131	1.5
Filler panel (Air Blocker)	22 x 127 x 333	0.6
Front Bezel (including Air Filter)	482 x 133 x 19	0.5

3.5 Mounting Options

You can install the system in a standard 19" ANSI rack using the rail kit.

Downloaded from Arrow.com.



⚠ CAUTION

Personal Injury
The system is heavy and improper handling may lead to muscle strain or back injury. Two member team is required to lift the system or use lifting aids and proper lifting techniques when handling the system. Do not use the FRU handles to lift the shelf.

Personal Injury or System Damage
A top-heavy rack can topple over, causing damage to equipment and injury to personnel.
If your system is the only one in the rack, make sure to mount the system in the lowest part of the rack. If several systems are installed in one rack, start with the heaviest component at the bottom. If the rack is equipped with stabilizing devices, make sure that they are installed and extended so that the rack is secure. Then proceed to mount or service the system.

NOTICE

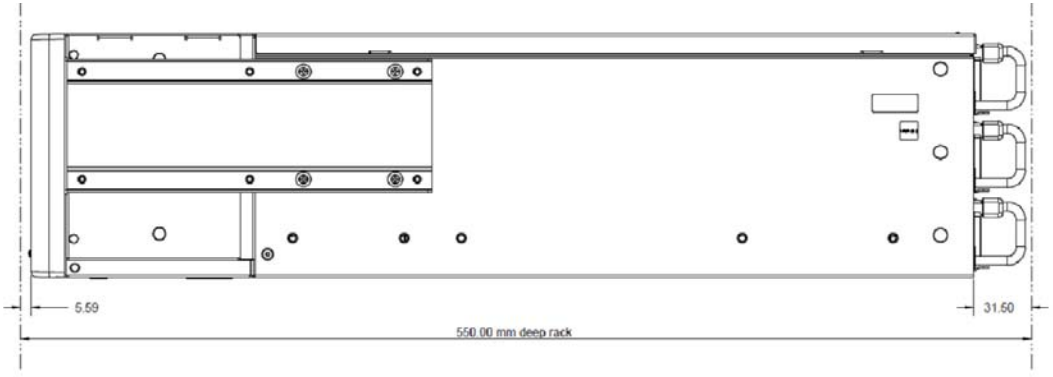
Product Damage
During the course of handling, shipping, and assembly, pins, mounting screws, fans and other items can become loose or damaged.
Do not operate a damaged system, this can cause damage to devices that interfere with it.

Grounding
If the product is not properly grounded, it may be damaged by electrostatic discharge. Make sure that each of the system's parts contact the EMI gasket. The system contains gaskets at the shelf and module level.
The shelf is also fitted with ESD snaps for the use with conductive wrist straps. Please take care for proper ESD protection of the operator.

Downloaded from Arrow.com.

You have to keep the following clearances when installing the system into a 550 mm deep rack. The physical dimensions in the figure below are in millimeters.

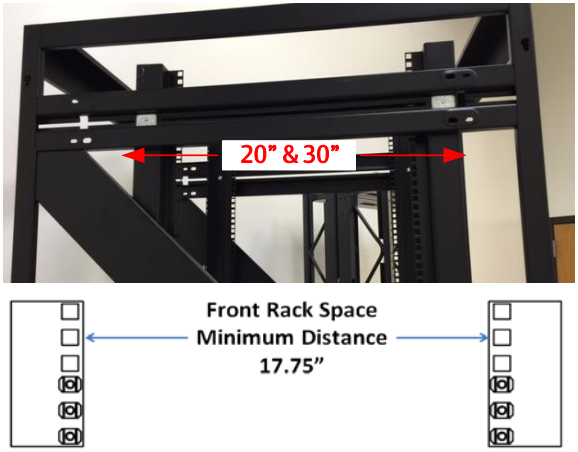
Figure 3-1 Rack Mounting Dimensions



3.5.1 MaxCore Rackmount Slides Installation

The rail kit explained in the section will only work with rack posts that are 20” to 30” inches apart. Deeper racks will require a special extension kit.

Figure 3-2 Rack posts - 20” and 30”



Downloaded from Arrow.com.

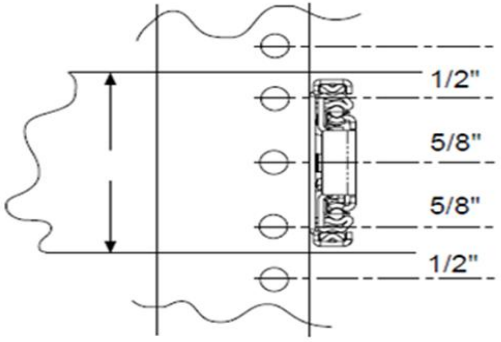
Equipment racks with tapped holes will not work for this installation.

The rack must have square or round holes that will allow the rail brackets to be mounted behind the rack rails for the screws to go through the opening and thread into the pressed-in nuts mounted into the rail mounting brackets.

Rack rails are not part of the MaxCore package. You need to order rails (P/N:MC3000-RAIL) separately. See *Ordering Information* on page 51.

For 2U to 4U spacing, slides can mount to chassis at various locations relative to the EIA rail 1/2", 5/8", 5/8" pitch pattern as shown in the following figure.

Figure 3-3 EIA Rail Spacing



Downloaded from Arrow.com.

The rail kit comprises following components as shown in the below table.

Table 3-7 Components in Rail Kit

Component	Quantity
Rack Member Assembly with Chassis Member Rail	1
Rear Long Bracket	2 (Part number - 0706829G01x)
Front Short Bracket	2 (Part number - 0706829G02x)
Chassis/Rail Screws	12 (# 8-32) (Part number - 0306856B01x)
Rack/Rail Thumb Screws	8 (# 10-32) (Part number - 0306857B01x)

Downloaded from Arrow.com.

MaxCore Rack Mount Slides Installation

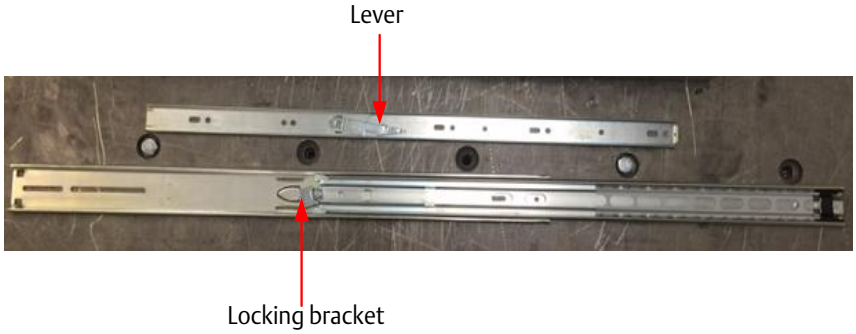
To install a MaxCore system into a rack, perform the following steps:

1. Slide out the Chassis Member Rail and release it from the Rack Member Assembly.

Rack Member Assembly with Chassis Member Rail

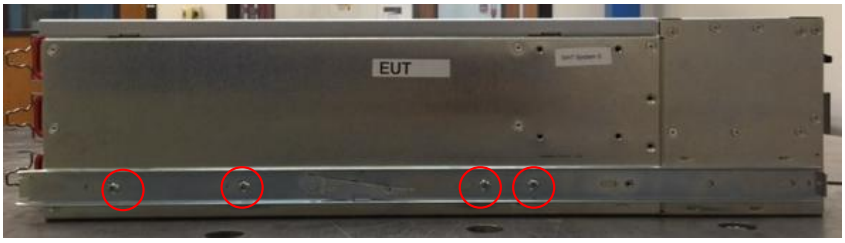


2. Align the locking bracket to collapse Rack Member Assembly and then press upwards or downwards to release and pull out Chassis Member Rail.



Downloaded from Arrow.com.

3. Attach Chassis Member Rail to both sides of the MaxCore system using the chassis/rail screws included in the kit.



Chassis/Rail Screws (on both sides of Chassis)

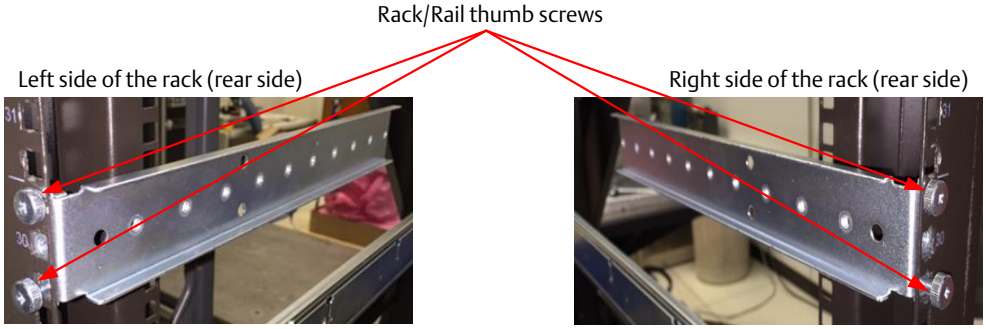




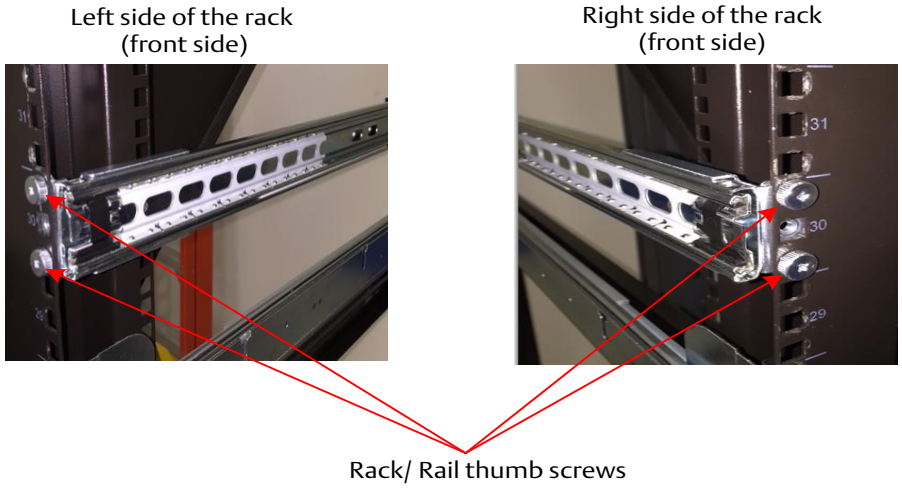
Chassis Member Rail edge must be behind the MaxCore front edge

4. Install Rear Long Brackets to both sides of the rack to the rear side using the rack/rail thumb screws included in the kit.

Downloaded from Arrow.com.



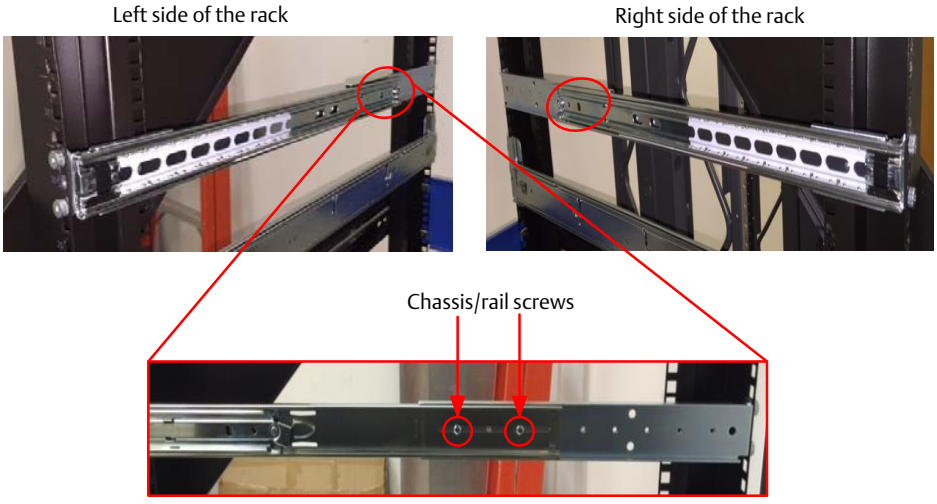
5. Install Rack Member Assembly (with Short Bracket pre-installed) on both sides to the front side of the rack using rack/rail thumb screws included in the kit.



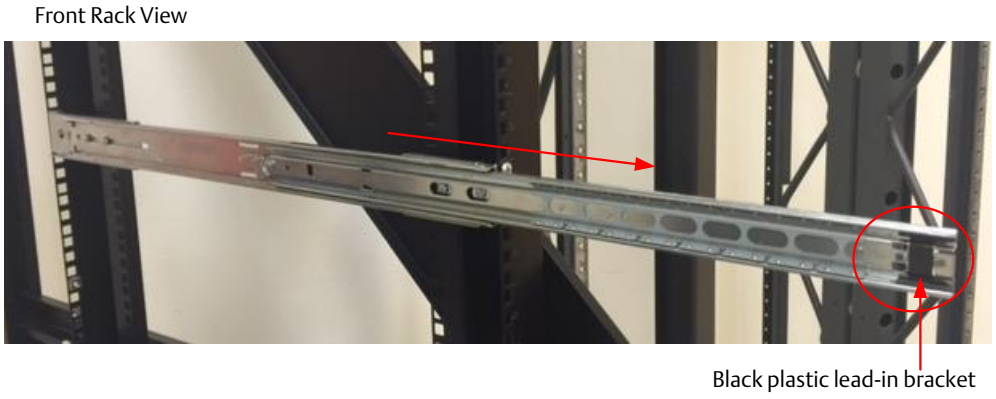
Do not tighten the screws at this point of time.

Downloaded from Arrow.com.

6. Press the rail into the rear bracket firmly and install the chassis/rail screws on both sides.



7. On the front side of the rack, extend the slides to fully locked position and bring ball retainer on both the sides. After that, align rail with the black plastic lead-in pins.

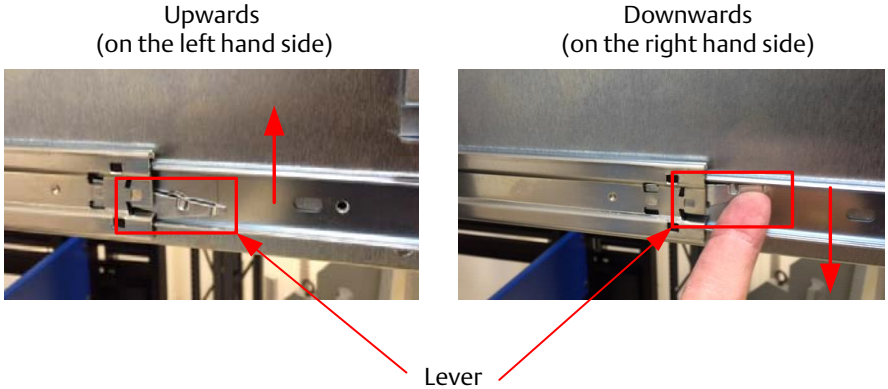


8. Lift the MaxCore system with the Chassis Member Rails installed and align both sides of the rails into the black plastic lead-in bracket from both sides and push the chassis back until it locks.

Downloaded from Arrow.com.

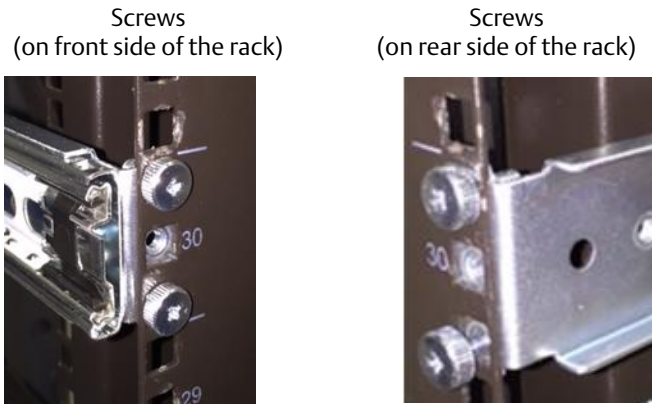
Note: A two-person effort is required for this operation due to weight and alignment needs.

9. Slide MaxCore system into the rails until it locks.
   Lift the lever on the left hand side upwards and the lever on the right hand side downwards to unlock and then slide the chassis back into the rack position.



10. Check slide alignment by sliding chassis constantly backward and forward.
    Note: Any sign of binding indicates lateral stress or misalignment. Adjust slide position until movement is smooth.

11. Loosen screws from both front and rear sides until the system slides without binding.

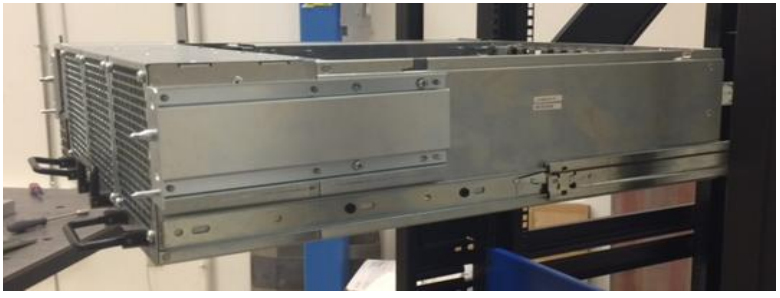


Downloaded from Arrow.com.

Inserting and locking MaxCore System

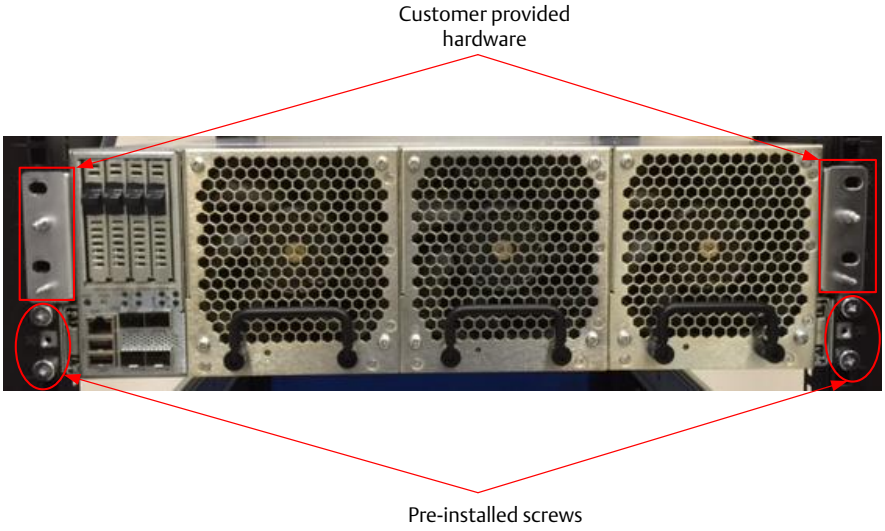


Checking slide alignment



12. Secure MaxCore system to the rack using customer provide hardware on both sides and also secure rails by tightening the pre-installed screws on both sides (on both front and rear sides).

Downloaded from Arrow.com.



This completes the MaxCore system installation into a rack.

3.6 Cooling Considerations

The MC3000 provides fault-tolerant cooling based on three fan modules located at the front of the system underneath the snap-in system front bezel. Each module houses two fans. The airflow direction is from front to rear in the chassis.

The actual cooling performance may depend on the PCIe card slot population and the heat-sink design of the installed cards. It should be validated based on the used system configuration.

The distance to other equipment must be sufficient to avoid overheating of the system.

If you install the system into a closed frame, ensure that the air inlet and outlet are kept free.

Downloaded from Arrow.com.

3.7 Acoustic Noise Control

This system has a built-in noise control due to the fan speed control. If the system is installed in an environment where the noise may be harmful to personnel being exposed to the noise during extended time periods, additional protective measures should be considered.

Downloaded from Arrow.com.

This chapter provides information on installation and removal of PCIE cards, procedure for covering unused slots, replacing AC or DC power supply units, replacing fan modules, installing disk drives, and maintenance of air filters. Also, the status of LEDs while installing and removing the card are described in this chapter.

4.1 Installing and Removing PCIE Cards

The installation and removal procedures of PCIE cards depend on the type of the card. Refer to the documentation of the respective PCIE card for these procedures.

In order to install or remove a PCIE card in the MC3000 system, first shut down the system, disconnect from AC or DC power, and remove the housing cover of the system.

The system can be shut down through the system's BMC or through Artesyn's SSF running on MaxCore.



⚠ CAUTION

Do not operate your equipment with the cover removed.
Allow the equipment to cool before removing the cover or touching internal components. PCIE cards and other components in the system may become hot during normal operation.
Use care when removing PCIE cards after operation.

To open the housing cover of the MC3000 system, push the lock button in the middle of the housing cover and push the housing cover towards the rear of the system. The cover will slide backwards and can be lifted off the system.



The system will ship with filler cards or filler panels installed into unpopulated PCIe slots. You have to remove the filler cards or filler panels before installing PCIE cards.

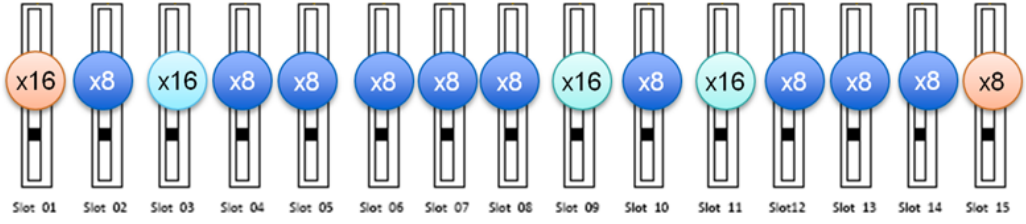
Downloaded from Arrow.com.

⚠ CAUTION

Product Damage
Removing or adding a PCIE card from the system while the system is powered up may damage the PCIE card and the system.
Whenever removing or adding a PCIE card from the system, power down the system first and disconnect it from AC or DC power.

You can access all 15 PCIe slots of the MC3000 system and may add or remove PCIE cards. Four of the 15 PCIe slots are x16 slots, whereas the remaining other slots are x8 slots. The following figure shows the capabilities of the slots.

Figure 4-1 MaxCore PCIe Slots



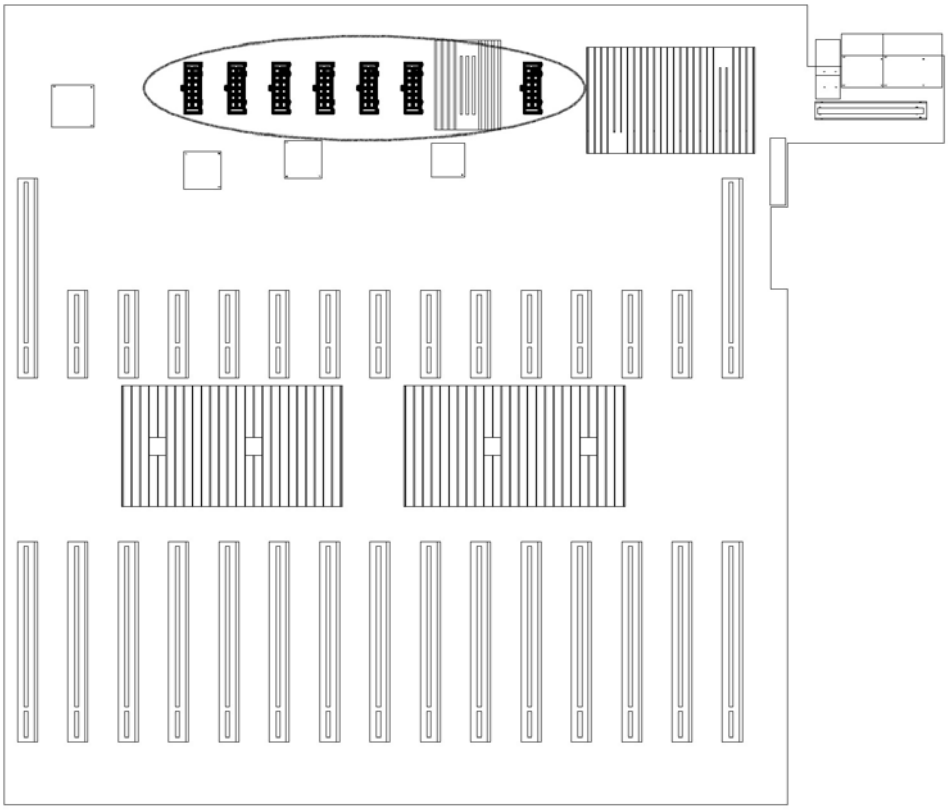
To connect these cards with the Aux power, you need to order a cable MC3000-ACC-CBL (connects a single PCIE card) or MC3000-ACC-Y-CBL (connects two PCIE cards) from Artesyn separately.

There are seven Aux power connectors available in the MaxCore system. In case more than seven PCIE cards need to get connected to AuxPower, two cards which are placed adjacently can be supplied power from one AuxPower source using the MC3000-ACC-Y-CBL. For more information about cables, refer to the section *Ordering Information* on page 51.

Downloaded from Arrow.com.

Figure 4-2 shows the location of AuxPower connectors in the MaxCore system.

Figure 4-2 Location of AuxPower Connectors in MaxCore System



Depending on the power dissipation and/or the thermal performance of a PCIE card, it may be necessary to add a PCIE filler card in the slot next to this card, if that slot remains empty.

All unused slots of the system must have Artesyn approved filler cards or filler panels. PCIE filler cards for the MaxCore system can be purchased from Artesyn.

After insertion or removal of a PCIE card make sure to attach the housing cover back and close it properly before reconnecting power to the system.

Downloaded from Arrow.com.

4.2 Replacing AC Power Supply Units

This section provides the information needed to replace the power supply units.

The system is equipped with up to three PSUs.They are installed on the right side of the system's rear. Before replacing a PSU, verify that a second PSU is present with its Green notification LEDs lit and that the remaining PSU(s) are capable of providing sufficient power to the respective system configuration.

If no other PSU is installed or operational, you have to power down the system before exchanging the PSU (see section *Powering Down the System* on page 112).

NOTICE

Damage of Circuits
Electrostatic discharge and incorrect card installation and removal can damage circuits or shorten their life.
Before touching the card or electronic components, make sure that you are working in an ESD-safe environment.

Replacement Procedure

To replace a PSU, proceed as follows:



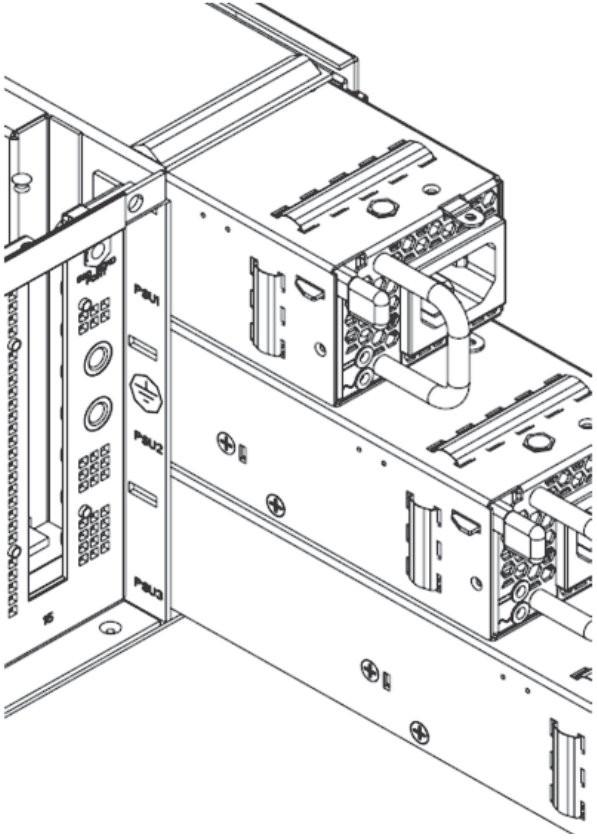
⚠ CAUTION

Personal Injury
Hot PSUs may cause injury.
Allow the PSU to cool before servicing.

1. Put on an ESD wrist strap.
2. Connect the strap to the system by attaching the front or rear ESD jack/ESD snap.
3. Switch the external disconnect device of the PSU to be replaced to the OFF (tripped) position, if it is not already in this position.

Downloaded from Arrow.com.

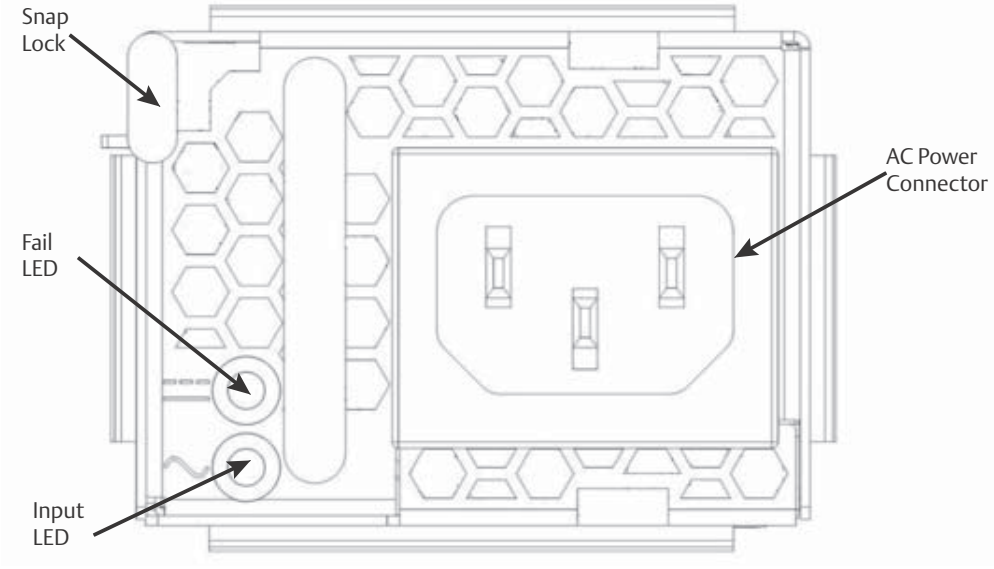
4. Push the Power Supply's snap-in lock sideways and pull the PSU handle.
5. Remove the PSU from the system bay by pulling the PSU handle.
6. Insert the replacement PSU.



7. Carefully push the PSU all the way in until the snap-in lock engages.
8. Reconnect the power cable.
9. Turn on the feed power, if it is not already turned on.

Downloaded from Arrow.com.

10. Check the PSU status LED and take the appropriate actions as listed in the table below.



PSU Status LED	LED Status	
	Input LED (Green)	Fail LED (Amber/Green)
AC power is disconnected. Action: Turn off the feed power and attach the power cable at the power connector.	Off	Off
AC input present, STBY ON, main output OFF	On	Blinking Amber (at least 1 Hz)

Downloaded from Arrow.com.

PSU Status LED	LED Status	
Main output ON	On	On, Green
Power supply warning (hi-temp)	On	Blinking Amber/Green, at 2:1 duty ratio, least 1 Hz
Power supply warning (slow fan)	Off	Blinking Amber/Green, at 1:1 duty ratio, least 1 Hz
Power supply failure (OVP, OTP, FAN FAULT)	On	On, Amber

4.3 Replacing DC Power Supply Units

This section provides the information needed to replace the Power Supply Units (PSUs). The system is equipped with up to three PSUs. They are installed at the right side of the system's rear.

Before replacing a PSU, verify that at least a second PSU is present with its Green notification LEDs lit and that the remaining PSU(s) are capable of providing sufficient power to the respective system configuration.

If no second PSU is installed or operational, you have to power down the system before exchanging the PSU (see section *Powering Down the System* on page 112).

NOTICE

Damage of Circuits
Electrostatic discharge and incorrect card installation and removal can damage circuits or shorten their life.
Before touching the card or electronic components, make sure that you are working in an ESD-safe environment.

System Damage
Inserting or extracting the PSU with the PSU breaker in the ON position may damage your system.
If power is connected to the system, make sure the PSU breaker is in the OFF position before you insert or extract a PSU.

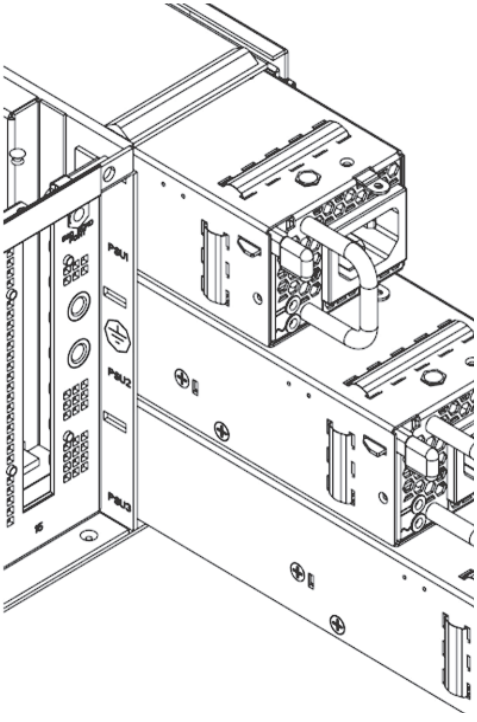
Downloaded from Arrow.com.

Replacement Procedure

To replace a PSU proceed as follows:

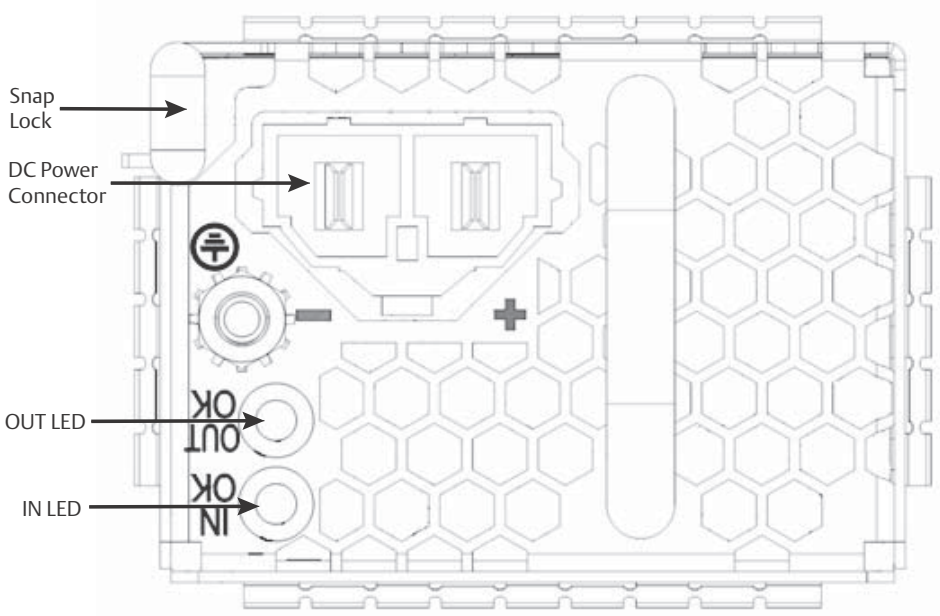
	**⚠ CAUTION** **Personal Injury** **Hot PSUs may cause injury.** **Allow the PSU to cool before servicing.**

1. Put on an ESD wrist strap.
2. Connect the strap to the system by attaching the front or rear ESD jack/ESD snap.
3. Remove the PSU from the system by pulling the PSU handle.
4. Insert the replacement PSU.



Downloaded from Arrow.com.

5. Check the PSU LEDs and take the appropriate actions as listed in the table below.



PSU Status	LED Status	
	Input LED	Output LED (Amber/Green)
DC power is disconnected. Action: Turn off the feed power and attach the power cable at the power connector.	Off	Off
DC input present, STBY ON, main output OFF	On	Blinking Amber (at least 1 Hz)
Main output ON	On	On, Green
Power supply warning (hi-temp)	On	Blinking Amber/Green, at 2:1 duty ratio, least 1 Hz
Power supply warning (slow fan)	Off	Blinking Amber/Green, at 1:1 duty ratio, least 1 Hz
Power supply failure (OVP, OTP, FAN FAULT)	On	On, Amber

Downloaded from Arrow.com.

NOTICE

PSU Damage
Applying reverse power causes damage to the electrolytic capacitors of the filter. Therefore, only switch on the breakers, if no Red light is visible.

4.4 Maintaining Air Filters

Routine filter maintenance is required to ensure that the system operates efficiently. The following section provides the information needed to replace and store air filters.

Downloaded from Arrow.com.

4.4.1 Replacing the Air Filter

The system is equipped with an air filter which is located within the system's front bezel.

NOTICE

System Damage
Air Filters
Air contamination can pollute the air filters and obstruct the air intake of the system which may cause system overheating and component damage.
To guarantee proper airflow through the system the air filters have to be replaced at least every six months. Artesyn recommends to replace the air filters every 90 days. Filter replacement frequency depends on the environment the system is subjected to. Because central offices vary in physical location and cleanliness, check your air filters every week after you first install your system. In a dusty environment, filter replacement may be required more often than in a cleaner environment. Check the filters frequently until you have a good idea of how often they must be replaced. Based on your findings, establish a regular replacement schedule and keep a log to record the date of each filter replacement.

Filter Frames
Wrong insertion may damage the frame or the guides.
When inserting the filter frame into the system, pay attention to insert the appropriate bottom or top frame and to align it accurately to the guides.

Damage of Circuits
Electrostatic discharge and incorrect installation and removal of the product can damage circuits or shorten their life.
Before touching the product make sure that your are working in an ESD-safe environment or wear an ESD wrist strap or ESD shoes. Hold the product by its edges and do not touch any components or circuits.



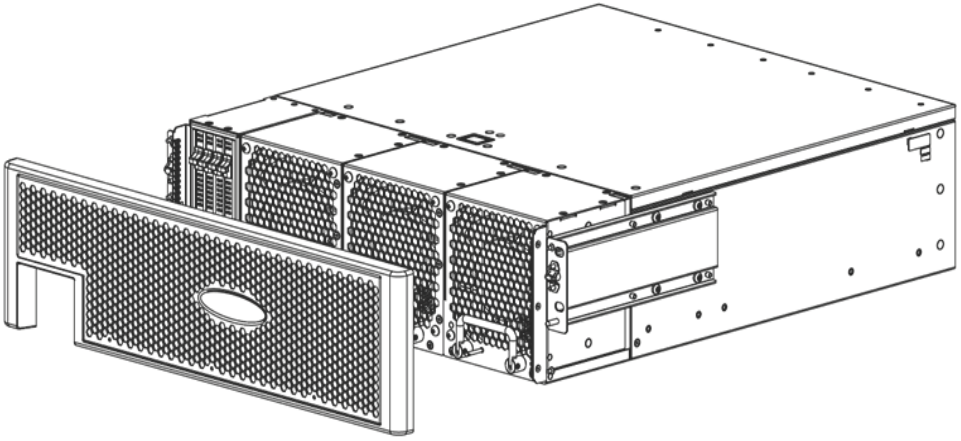
You can order replacement filters from Artesyn. For details refer to Table "Ordering Information" on page 51.

Downloaded from Arrow.com.

Replacing the Top Air Filter

To replace the top air filter, proceed as follows:

1. Make sure that the replacement filter is available.
2. Remove the front bezel, if it is not already removed.



3. If necessary, use compressed air to clean the dust from the fan modules.
4. Detach the air filter from the frame.
5. Attach the new filter and align it accurately to the frame.
6. Press the air filter to the hook-and-loop fastener on the frame.
7. Put the front bezel with the new filter back onto the front of the system. Push the bezel until the snap-in locks engage.

4.4.2 Storing the Air Filters

It may be best to keep extra filters on hand so that you can exchange them without delay when necessary. The ideal storage condition is a cool and dry environment. High temperature and humidity adversely affect the filters. Foam degrades when exposed to solvents and sulfates, such as engine exhaust.

Downloaded from Arrow.com.

Ensure that the relative humidity is between 40% - 80% and the temperature is between 4.4 °C - 32.2 °C (40 °F - 90 °F). Keep the air filters dry.



Artesyn does not recommend storing foam filters for many months or years at a time. Purchase enough to keep adequate inventory, but do not store them not more than a few months.

4.5 Replacing Fan Modules

The following section provides the information needed to replace the fan trays. The fan trays are located on the front of the system behind the air filter and front bezel.

NOTICE

System Damage
Insufficient cooling may damage the system.
The cooling system is designed to provide sufficient cooling with a single fan module removed. However, under bad conditions or due to a failure of the remaining fans, the cooling capacity of the remaining fan modules may not suffice.
Avoid delays during fan replacement.

Fan Damage
When a fan module is taken out of operation or is removed during a replacement procedure, the system management controller will compensate for the loss by increasing the speed of the remaining fans. Turning on high speed for a long time may shorten the life of the fans and may exceed allowable acoustic noise limits.
Replace the fan module without delays.

System Damage
Removing more than one operating fan module will lead to overheating very quickly.
Make sure that there is always only one operating fan module removed from the system.

Downloaded from Arrow.com.

NOTICE

Damage of Circuits
Electrostatic discharge and incorrect installation and removal of the product can damage circuits or shorten their life.
Before touching the product make sure that you are working in an ESD-safe environment or wear an ESD wrist strap or ESD shoes. Hold the product by its edges and do not touch any components or circuits.

Replacing Fan Modules

The procedure for replacing is the same for all fan modules.



Unless an internal fuse has blown (not field replaceable), fan modules are never actually powered down.

The fan rotation can be stopped by the BMC.

If the control board has failed, fans will be operating at 100% speed.



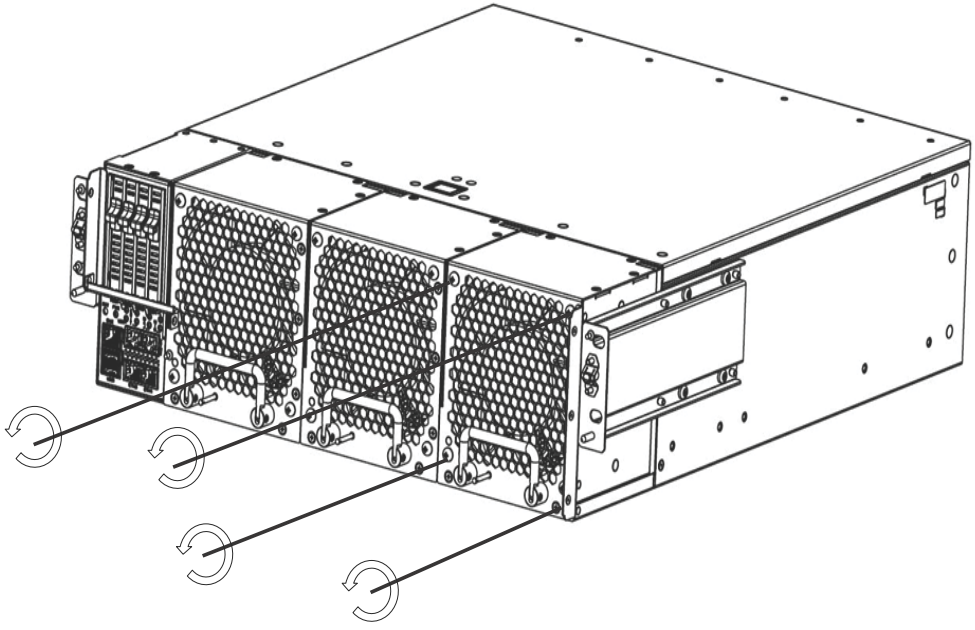
⚠ CAUTION

Personal Injury
Rotating Fans
Inserting tools or fingers into operational fans may cause injuries.
Keep clear of the fans as long as they are rotating.

Downloaded from Arrow.com.

To replace a fan module:

1. Remove the replacement fan module from the shipping box and make sure that it is the correct model for the system (see *Ordering Information* on page 51).
2. Remove the front bezel with the air filter from the system by pulling it out of the snap-in locks at the left and right side of the bezel. Unfasten the four mounting screws of the fan module to be replaced.



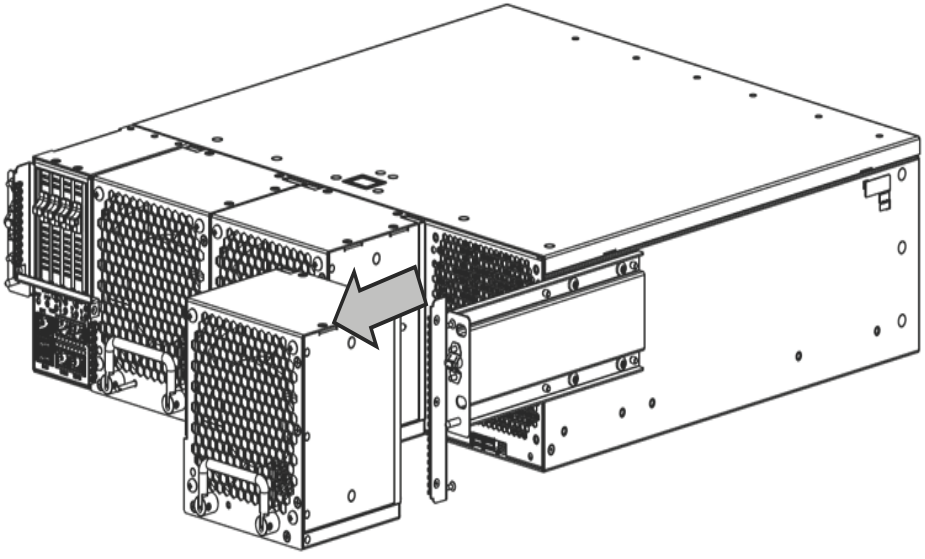
3. Grasp the handle and pull the fan module carefully out of the system.



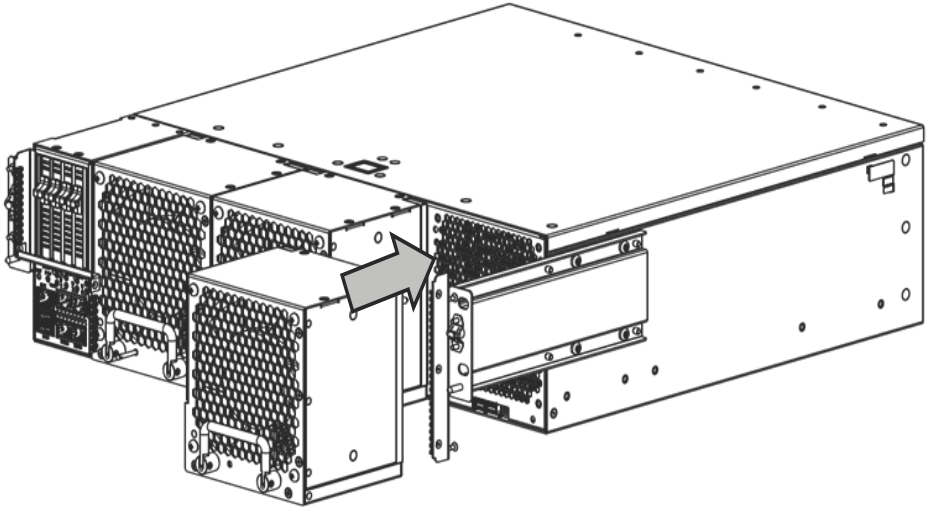
⚠ CAUTION

Personal Injury
Rotating Fans
Inserting tools or fingers into operational fans may cause injuries.
Keep clear of the fans as long as they are rotating.

Downloaded from Arrow.com.

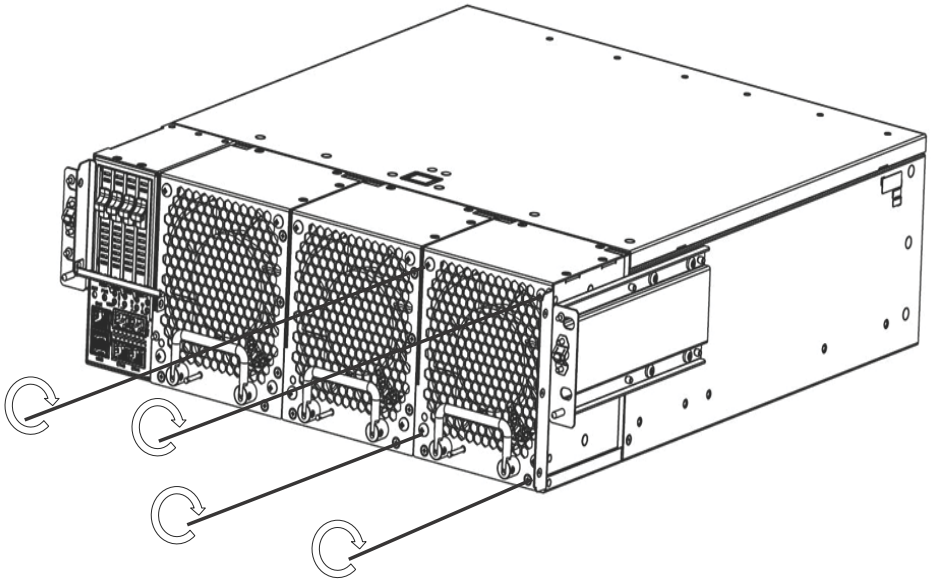


4. Take the replacement fan module and insert the fan module carefully into the system while keeping it in a horizontal position. Allow the fan module connectors to mate smoothly.



Downloaded from Arrow.com.

5. Fasten the four mounting screws of the fan module.



6. Query the BMC to ensure the fan module is operating properly.

4.6 Installing Disk Drives into MaxCore Platform

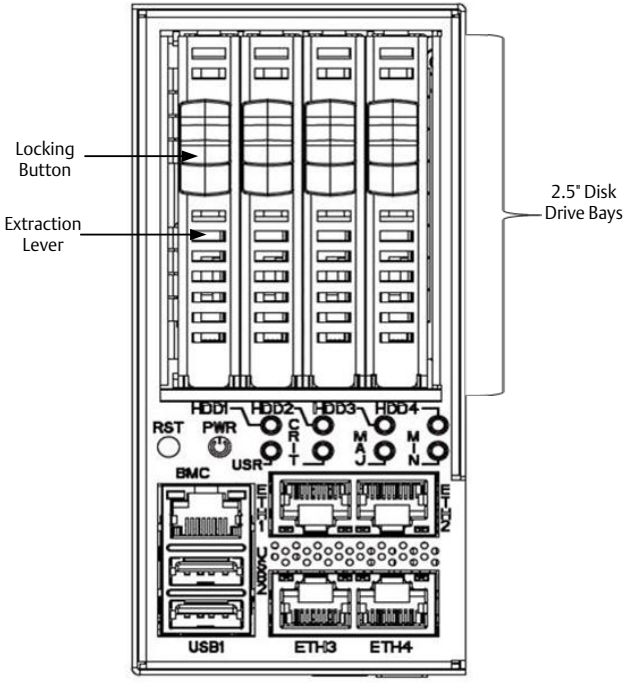
The MaxCore system supports four 2.5” hot-swap capable disk drive bays to allow 2.5” SATA HDDs or SSDs. The standard Artesyn MaxCore MC3000 platform is shipped without any 2.5” disks pre-installed. Artesyn offers SSD kits (currently 512 GB and 1TB, see *Ordering Information on page 51*) that can be installed into the MaxCore MC3000 platform. To install a disk into the MaxCore system or remove from it, follow the below steps:

Downloaded from Arrow.com.

Extract Disk Drive from Drive Bay

To extract the disk drive from a drive bay in a MaxCore system, perform the following steps:

1. Remove the front bezel, including the air filter by pulling it off its snap-in bolts (see section *Replacing the Air Filter* on page 85).
   After removing them, on the left side of the system, right above the IO panel you will find the four disk drive bays as shown in the figure below.



2. Push the black locking button of the respective bay downwards and then pull it backwards. This will open the disk extraction lever.
3. Grab the extraction lever and pull the entire disk drive carrier off the slot.

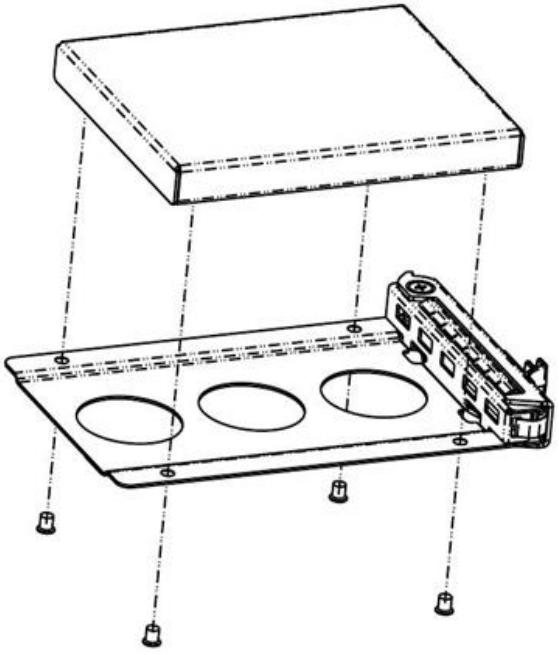
Downloaded from Arrow.com.

Assemble or Replace Hard Disk Drive

If no disk drive had been previously assembled, the disk drive carrier will have a metal filler assembled, instead of a disk drive.You need to remove the metal filler from the carrier, before assembling a disk drive to the carrier. If a disk drive had already been installed to the carrier, you may need to replace the disk drive. In either case (metal filler assembled or disk drive assembled) the steps to remove and assemble a disk drive are the same.

The following steps help you to assemble or replace a disk drive from drive bay in a MaxCore system:

1. Unscrew the four screws on the bottom of the carrier that keep the filler or the disk drive in place, as shown in the below figure.



Retain the four screws for mounting the required disk drive.

Downloaded from Arrow.com.

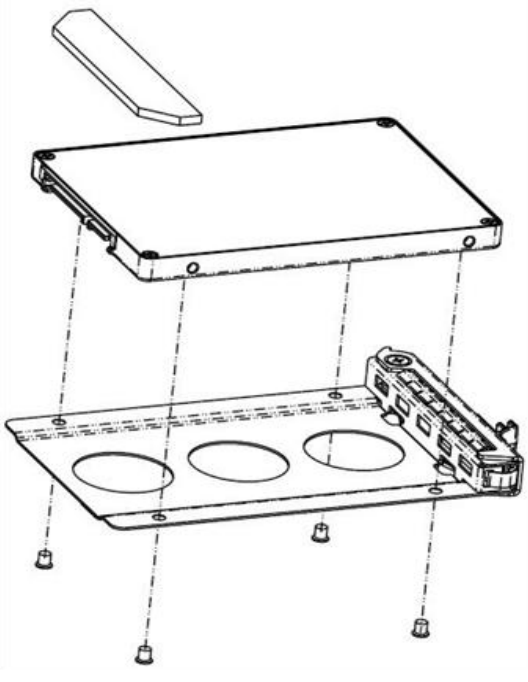
2. Place the 2.5” SATA disk drive onto the carrier with the SATA connector at the opposing side to the extraction lever. Align the mounting holes of the carrier with the threaded holes of the disk drive and then insert and fasten the four screws securely.

The MaxCore disk drive bays are designed to fit 9.5 mm thick disk drives. If a 7 mm disk drive is used, an additional 7-to-9.5 mm-spacer on top of the disk drive is required to compensate the disk’s thickness. Without that spacer the carrier with the disk will not properly mate with the MaxCore internal SATA connector upon disk carrier insertion, which may even damage the connector.

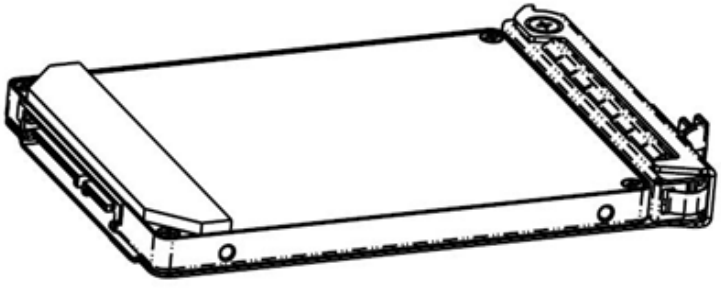
The Artesyn HDD kits containing 7 mm thick HDDs come with a self-adhesive spacer (see *Ordering Information* on page 51) that needs to be put on the rear top (on top of the disk connector) of the mounted disk as shown in the below figure.

Downloaded from Arrow.com.

3. To insert a 7 mm disk drive into the drive bay, first remove the protection foil from the spacer, carefully align the spacer with the adhesive side down towards the disk and press firmly.



The disk assembled to the carrier with the 7-to-9.5mm-spacer attached will look as shown in the following figure.



Downloaded from Arrow.com.

Insert Disk Drive into Drive Bay

The following steps help you to insert a disk drive into drive bay:

1. Insert the carrier with the disk back into the respective disk drive bay of MaxCore and carefully close the extraction lever.
2. Put the MaxCore front bezel back onto the system. Carefully push it back onto the snap lock bolts (see section *Replacing the Air Filter* on page 85).

Downloaded from Arrow.com.

This chapter provides information on the cooling system and the fan modules.

5.1 Cooling Subsystem

The BMC provides cooling management to the MC3000 system to keep the system cool under normal operation conditions. The BMC adjusts the fan levels to adapt to the changing conditions of the system elements or environment.

The MC3000 provides fault-tolerant cooling based on three fan modules, each of them containing two independent fans. The fan modules are located at the front side of the system. The airflow direction in the system is from front to rear. The proper operation of each fan module is indicated by respective LEDs on the front bezel.

Actual cooling performance also depends on the card slot population and the heatsink design of the installed PCIe cards and should be validated based on the used system configuration.



The distance to other equipment must be sufficient to avoid an overheating of the system.

Each of the fan modules contains two independent fans. Individual fan failures are detected by monitoring the fan rotation speed.

The BMC controls the fan speed based on sensor and failure information acquired from fan and system sensors. Usually, the cooling system runs the fans at speed levels between 15% and 75%, depending on ambient temperature and system configuration.

Since commercially available PCIe cards do not provide a standardized method for monitoring the cards temperature from the respective host CPU, Artesyn provides a concept for the system integrator to integrate temperature monitoring of third party PCIe cards into the cooling management of the MC3000 system.

For further information about this concept and how to integrate it, please contact your local Artesyn Sales representative.

Downloaded from Arrow.com.

Downloaded from Arrow.com.

This chapter provides instructions for installing and removing the system in a rack. It also provides information and procedures for grounding the system, powering up the system, powering down the system, and disconnecting the system from power feed.

6.1 Before Installation

This section details the necessary equipment and information required for system installation.

6.1.1 Tools Required

Before you start the installation, make sure that you have all the necessary equipment at hand.

Usage	Equipment
General	• Phillips head screwdriver #1, #2, and #3 (Large, medium and small) • Wrenches 7, 8, and 10 mm • ESD wrist strap • Anti-static mat
Shelf	Transport equipment: Hand truck or forklift/pallet truck Lifting equipment for installation
Grounding	Earth grounding cable with a two-hole lug, distance 5/8" (15.9 mm) **Note**: Grounding cable of size 1.25mm^2 for AC system and 2.5 mm^2 for DC system.
AC PSU	Power input cables with a minimum cross section of 1mm^2
DC PSU	Power input cables with a minimum cross section of 2.5 mm^2, AWG 12
System Access	Crossover cable Twisted pair Ethernet cable CAT-5

Downloaded from Arrow.com.

6.1.2 Torque Values

In the following table, you can find information on the torque values that you have to use while handling and maintaining the system.

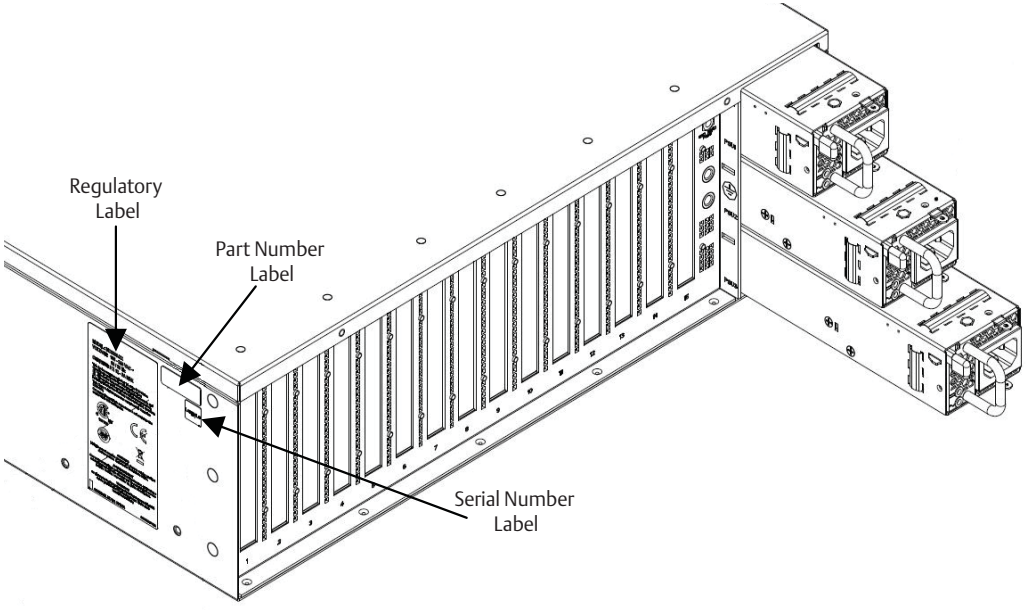
Table 6-1 Torque Values

For...	Value	
	Nm	**in lbs**
Ground nuts	2.5	22.12
Pluggable screw terminals	0.6	5.31
Thumb screws for FRUs	0.6	5.31

6.1.3 Type Label Location

The serial number label for the system is located at the system's right hand side.

Figure 6-1 Serial Number Label Location



Downloaded from Arrow.com.

6.2 Installation

Ensure that the requirements outlined in the section *Requirements* on page 57 are met.

While installing the system, observe the following general safety notes and precautions.

NOTICE

- **Installation codes**
  This unit must be installed in accordance with the National Electrical Code (NEC).
- **Conductor ampacity**
  According to UL 60950, Annex NAE (NEC Article 645-5(a)), the branch-circuit conductors supply must have an ampacity of not less than 125% of the total connected load. Per NEC Article 310-15 and Table 310-16, the minimum American Wire Gauge (AWG) has to be selected.
- **Overcurrent protection**
  A readily accessible listed branch circuit overcurrent protective device must be incorporated into the building wiring. For appropriate AWG rating of the overcurrent protection device, see NEC Table 310.16 and other national regulations.
  AC PSU input is fused at 16 A. External wiring and circuit interruption should be sized accordingly.



Artesyn is not responsible for regulatory compliance or malfunction of any user-modified product.

Downloaded from Arrow.com.

NOTICE

System Damage
Environmental contamination can impair system operation. Locate the system in a stable area free of excess movement and jarring and free of dust, smoke, and ESD. Make sure that the temperature does not exceed the operating temperature given in the environmental requirements in this manual and allow room for proper air flow for cooling.

System Overheating
Cooling Vents
Improper cooling can lead to card and system damage and may void the manufacturer's warranty.
To ensure proper cooling and undisturbed airflow through the system always operate the system in a horizontal position. Do not obstruct the ventilation openings at the front and rear of the system. Keep the fresh air intake at the bottom-front side of the chassis completely clear. Make sure that the fresh air supply is not mixed with hot exhaust from other devices. Make sure that all slots are populated with either cards or filler cards.

6.2.1 Installing the System in a Rack

The following procedure describes how to install the system in a rack.



For MC3000 AC, use power input cables with a cross section (minimum) of 1 mm^2.

For MC3000 DC, use power input cables with a cross section (minimum) of 2.5 mm^2, AWG 12.

Downloaded from Arrow.com.



⚠ CAUTION

Personal Injury
The system is heavy and improper handling may lead to muscle strain or back injury. Have two people lift the system or use lifting aids and proper lifting techniques when handling the system. Do not use the FRU handles to lift the shelf.

Personal Injury or System Damage
A top-heavy rack can topple over, causing damage to equipment and injury to personnel.
If your system is the only one in the rack, make sure to mount the system in the lowest part of the rack. If several systems are installed in one rack, start with the heaviest component at the bottom. If the rack is equipped with stabilizing devices, make sure that they are installed and extended so that the rack is secure. Then proceed to mount or service the system.

NOTICE

System Damage
During the course of handling, shipping, and assembly, pins, mounting screws, fans and other items can become loose or damaged.
Do not operate a damaged system, this can cause damage to devices that interfere with it.

Grounding
If the product is not properly grounded, it may be damaged by electrostatic discharge. Make sure that each of the system's parts contact the EMI gasket. The system contains gaskets at the shelf and module level.
The shelf is also fitted with ESD snaps for the use with conductive wrist straps. Please take care for proper ESD protection of the operator.

Downloaded from Arrow.com.

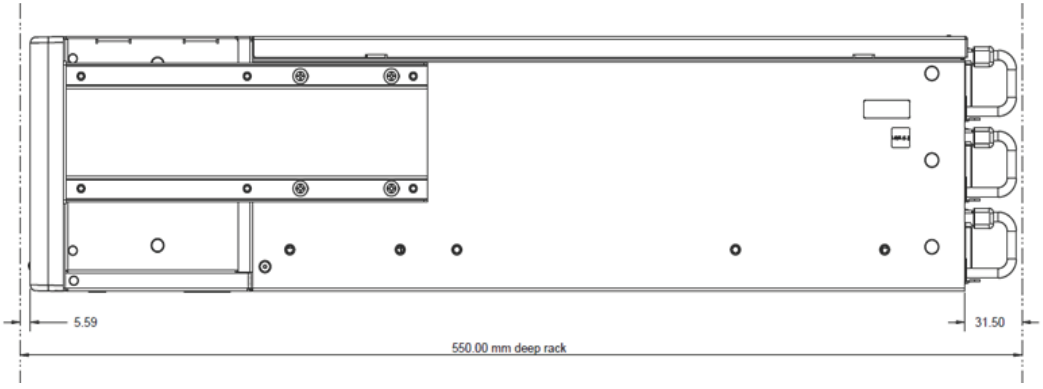
Procedure

To install a system into a standard 19" ANSI rack, proceed as follows:

1. Insert the system into a standard 19" ANSI rack.
2. Fasten the system to the rack via the integrated chassis mounting flanges using two bolts or screws (minimum 6 mm (0.24 inch) in diameter) on the left side and two on the right side of the system.
3. Make sure that the system has been placed in a location at room temperature for at least 24 hours before powering it up.

The following clearances are required when installing the system into an at least 550 mm deep rack. The physical dimensions in the figure below are in millimeters. Make sure that 60% of the rack's rear is open.

Figure 6-2 Rack Mounting Dimensions

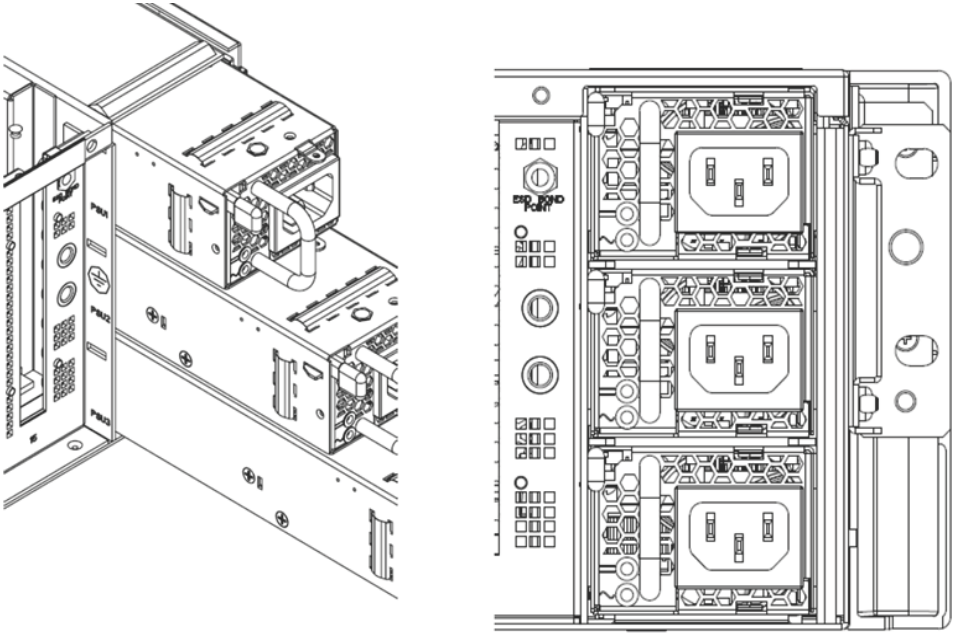


Downloaded from Arrow.com.

6.2.2 Grounding the System

This section provides information on how to provide grounding to the system.

Figure 6-3 System's Ground



Procedure

To ground the system:

1. Connect the rack ground lug to the M5 shelf ground at the right rear of the shelf and torque the shelf ground lug nuts to maximum, refer Table 6-1 for torque values. The lugs are marked with the corresponding grounding symbol. Artesyn recommends to use an earth grounding cable with a two-hole lug, behind (15.9 mm) in case of rack installation. Grounding cable of size 1.25 mm^2 for AC system, and 2.5 mm^2 for DC system.

2. Permanently connect the system to the earth ground of the building.

Downloaded from Arrow.com.

6.2.3 Powering Up the System

This section explains how to power up a system.



⚠ CAUTION

Personal Injury
Touching the PSU power input terminals with metallic objects on your hands, wrists, or hanging from your neck may lead to severe injuries through electric shock and burning.
Do not wear any metallic attire or commodity on your hands, wrists, or hanging from your neck when working at the power input terminals or power input cables. Be extremely careful when you use electrically conductive tools near the PSUs.

Short Circuit and Personal Injury
Ensure that the power feeds you plan to remove or attach are powered off and cannot be switched on when you are working.
Ensure that all power input lines are not energized. Be careful with the tools used in order to prevent a short circuit.

Personal Injury
Surfaces may get hot. Allow sufficient cool down period when removing FRUs with bare hands.

The following sections describe the startup procedure for MC3000 AC and MC3000 DC systems.

6.2.3.1 AC System Startup Procedure

Depending on the system configuration, the actual powering up may take up to 3 minutes.

Make sure that the system has been placed in a location at room temperature for at least 24 hours before powering it up.

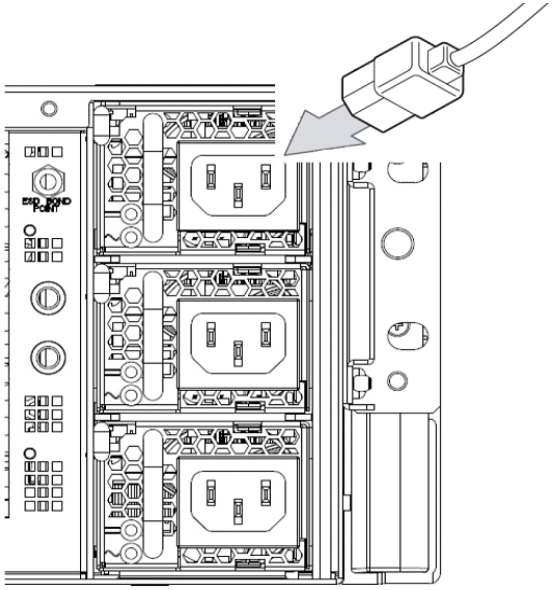
1. Put on an ESD wrist strap.
2. Connect the strap to the shelf by attaching the front or rear ESD jack/ESD snap.

Downloaded from Arrow.com.

3. Mount the grounding cable to the Protective Earth connection lug, if not done already.
4. Make sure that the external power feeds you plan to attach are powered off and cannot be switched on while you are working.
5. Connect the AC International Electric Code (IEC) wired connector to the AC power supplies.

NOTICE

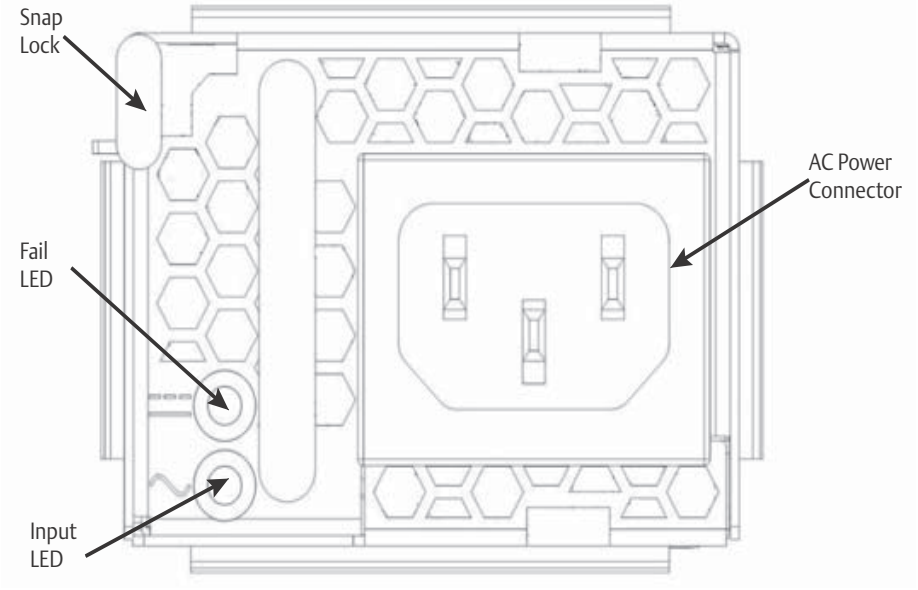
Product Damage
Improper cabling damages your product.



6. Turn on the external feed power.

Downloaded from Arrow.com.

7. Check the AC PSU Status LED and take the appropriate actions as listed in the table below.



PSU Status	LED Status	
	Input LED (Green)	Fail LED (Amber/Green)
AC power is disconnected. Turn off the feed power and attach the power cable at the power connector	Off	Off
AC input present, STBY ON, main output OFF	On	Blinking Amber (at least 1 Hz)
Main output ON	On	On, Green
Power supply warning (hi-temp)	On	Blinking Amber/Green, at 2:1 duty ratio, least 1 Hz
Power supply warning (slow fan)	Off	Blinking Amber/Green, at 1:1 duty ratio, least 1 Hz
Power supply failure (OVP, OTP, FAN FAULT)	On	On, Amber

Downloaded from Arrow.com.

6.2.3.2 DC System Startup Procedure

Depending on the system configuration, the actual powering up may take up to 3 minutes.

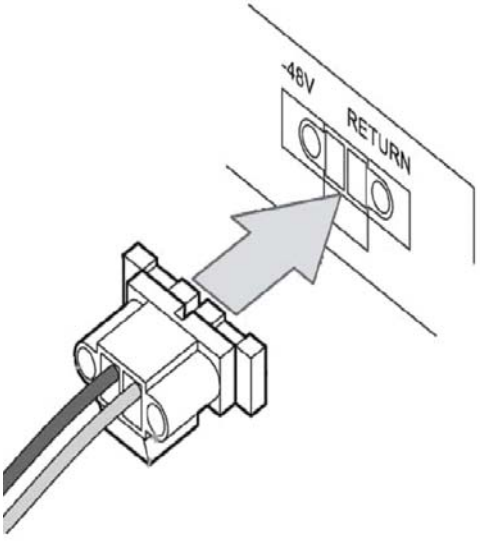
Make sure that the system has been placed in a location at room temperature for at least 24 hours before powering it up.

1. Put on an ESD wrist strap.
2. Connect the strap to the shelf by attaching the front or rear ESD jack/ESD snap.
3. Mount the grounding cable to the Protective Earth connection lug if not done already.
4. Make sure that the external power feeds you plan to attach are powered off and cannot be switched on while you are working.
5. Connect DC power cable with Molex connector 42816-0212 or any approved equivalent to the DC power supplies.

NOTICE

Product Damage
Improper cabling damages your product.
Take extreme care not to connect the power cable in reverse polarity.

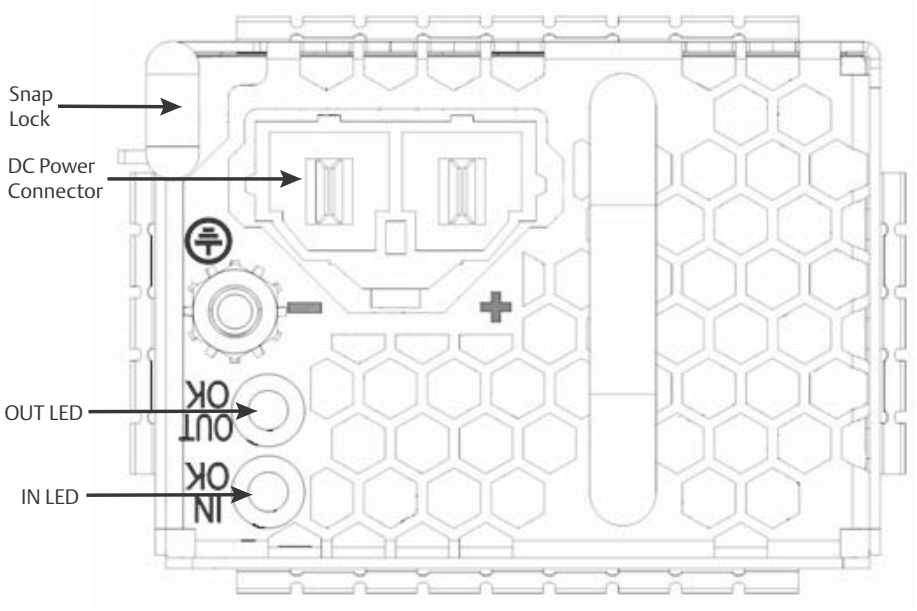
Downloaded from Arrow.com.



6. Turn on the external feed power.

Downloaded from Arrow.com.

7. Check the DC PSU LEDs and take the appropriate actions as listed in the table below.



PSU Status	LED Status	
	IN LED (Green)	OUT LED (Amber/Green)
DC power is disconnected. Turn off the feed power and attach the power cable at the power connector.	Off	Off
DC input present, STBY ON, main output OFF	On	Blinking Amber (at least 1 Hz)

Downloaded from Arrow.com.

PSU Status	LED Status	
	IN LED (Green)	OUT LED (Amber/Green)
Main output ON	On	On, Green
Power supply warning (hi-temp)	On	Blinking Amber/Green, at 2:1 duty ratio, least 1 Hz
Power supply warning (slow fan)	Off	Blinking Amber/Green, at 1:1 duty ratio, least 1 Hz
Power supply failure (OVP, OTP, FAN FAULT)	On	On, Amber

6.3 Removal

The following subsections describe the procedures for:

- Powering down the system
- Disconnecting a PSU from power feed
- Removing the system

6.3.1 Powering Down the System

For data integrity reasons Artesyn recommends to save data and close all applications before powering down the system.

Perform the system power down either through the BMC's web interface, the power button on the IO panel or through Artesyn's SSF. This will guarantee a clean shutdown of all system circuitries.

Do not disconnect AC or DC power to shut down the system. This may lead to improper start-up behavior when powering up the system again.

Downloaded from Arrow.com.

AC System Power-Down Procedure

To power down the AC system, proceed as follows:

1. Power down the system using system management software.
2. Remove power from the system utilizing the external disconnect.
3. Verify that the LEDs of the PSUs are off.



⚠ CAUTION

The system may be supplied with multiple power sources. Ensure to remove power from all sources to completely remove power from the system.

DC System Power-Down Procedure

To power down the DC system, proceed as follows:

1. Power down the system using a system management software.
2. Remove power from the system utilizing the external disconnect.
3. Verify that the LEDs of the PSUs are off.

6.3.2 Disconnecting the System from Power Feed

If you want to remove the system, you must disconnect it from power feed.

Downloaded from Arrow.com.

6.3.2.1 AC System Disconnection Procedure

To disconnect the system from power feed, proceed as follows:

1. Make sure that the power feeds you plan to remove are powered off and cannot be switched on while you are working.



⚠ CAUTION

Short Circuit and Personal Injury
Ensure that the power feeds you plan to remove or attach are powered off and cannot be switched on while you are working.
Ensure that all power input lines are not energized. Be careful with the tools used in order to prevent a short circuit.

2. To ensure that the PSUs are not energized, verify that the LEDs on the front of the power supplies are off.
3. Disconnect the AC power cords from the system.

Downloaded from Arrow.com.

6.3.2.2 DC System Disconnection Procedure

To disconnect the system from power feed, proceed as follows:

1. Make sure that the power feeds you plan to remove are powered off and cannot be switched on while you are working.



⚠ CAUTION

Personal Injury
Touching the PSU power input terminals with metallic objects on your hands, wrists, or hanging from your neck may lead to severe injuries through electric shock and burning.
Do not wear any metallic attire or commodity on your hands, wrists, or hanging from your neck when working at the power input terminals or power input cables. Be extremely careful when you use electrically conductive tools near the PSUs.

Short Circuit and Personal Injury
Ensure that the power feeds you plan to remove or attach are powered off and cannot be switched on while you are working.
Ensure that all power input lines are not energized. Be careful with the tools used in order to prevent a short circuit.

2. To ensure that the PSUs are not energized, verify that the **In** LEDs (in the middle) are off.

3. Disconnect the DC power cords from the system.

6.3.3 Removing the System



The system has to be powered down before the removal (see *Powering Down the System* on page 112).

Downloaded from Arrow.com.

Removing the System

To remove the system from a rack, proceed as follows:

1. Disconnect all power input cables.
2. Disconnect all cables from the PCIE cards and from the IO panel.
3. Remove the earth ground connection.
4. Loosen and remove the mounting screws.
5. Remove the system from the rack.

Downloaded from Arrow.com.

This chapter provides a detailed information on BMC operation and its maintenance, supported web interfaces, Serial Over LAN settings, Artesyn specific OEM commands, and on MaxCore firmware upgrade.

To have a quick understanding on how to bring up the system, refer to *MaxCore™ MC3000 Platform AC Quick Start Guide* manual.

7.1 Remote Management via Board Management Controller

The MaxCore platform provides a BMC that is dedicated to control and manage the system infrastructure and to provide a communication path to the management CPU (mCPU) for system configuration.

The BMC is a dedicated processor unit that monitors the MaxCore system using sensors and allows a remote administrator communicating with the system through an independent connection. The BMC is part of the Intelligent Platform Management Interface (IPMI) and is physically located on the backplane of the MaxCore system.

The sensors of the BMC measure internal physical variables such as temperature, power-supply voltage, fan speeds, communications parameters and functions. If any of these variables happens to stray outside specified limits, the administrator can take corrective action by remote control. The monitored device can be power cycled or rebooted as necessary.

In this way, a single administrator can remotely manage numerous systems simultaneously, saving on the overall operating cost of the network and helping to ensure its reliability.

The BMC core is implemented with the ASPEED AST2400 SoC and AMI MegaRAC® firmware.

7.1.1 Copyright Notice

This section contains information from MegaRAC (R) SP-X User Guide (Version 8) of AMI Megatrends Inc. For more information, you can download this document (DocID 430) from https://ami.com/en/resources/resource-library/?documentationSearch=user.

Downloaded from Arrow.com.

7.1.2 AMI MegaRAC® WEB GUI

The BMC provides a web interface, which can be accessed via RJ45 connector available at the front side of the platform (the default IP address is *192.168.201.9*).



If you are not able to access via RJ45 connector, it is possible that the IP address is changed. You can set the IP address to a custom default value, if any, or the factory default value (192.168.201.9) by pressing the reset (RST) button for more than 5 seconds.

The MegaRAC SP-X on SoC has an AMI generic, user-friendly Graphical User Interface (GUI) known as the MegaRAC GUI. It is designed for easy usage.This section allows you to become familiar with the various functions of MegaRAC GUI. Each function is described in detail in the following sections.

MegaRAC GUI supports almost all industry-specific web browsers, which include Internet Explorer, Firefox, Chrome, Opera, and Safari. You need to upgrade the browsers' versions, because some older versions of these browsers may not be compatible with MegaRAC GUI.

MegaRAC GUI is supported on Linux, Mac, and Windows operating systems.

Downloaded from Arrow.com.

7.1.2.1 Login Screen

The following screen appears, when you access the MegaRAC GUI using the BMC IP address. The BMC default IP address is 192.168.201.9.

Figure 7-1 Login Screen



Table 7-1 Login Page

Field or Button Name	Description
Username	Enter the username in this field. The default username is *admin*.
Password	Enter the password in this field. The default password is *admin*.
Login	After entering the required credentials, click this button to log on to MegaRAC GUI successfully.
Forgot Password	If you forget your password, you can generate a new one using this link. Enter the *username*, click the **Forgot Password** link. A new password is generated and sent to your configured or registered Email Id. This feature is only available after you have configured access to a mail server and after adding e-mail addresses to the user accounts.

Downloaded from Arrow.com.



The default user name and password are in lower-case characters. When you log in using your *username* and *password*, you get full administrative rights. It is advised to change your password once you login.



After you log into the application, it is recommended NOT to use the following options:

- **Refresh button of the browser**
- **Refresh menu of the browser**
- **Back and Forward options of the browser**
- **F5 on the keyboard**
- **Backspace on the keyboard**

7.1.2.1.1 Required Browser Settings

The following are the list of required browser settings:

- **Allow pop-ups from this site** - Indicates whether the browser allows popup for this site or not.
- **Allow file download from this site** - Allows file download for *Internet Explorer*, Choose **Tools** > **Internet Options** > **Security** Tab, based on device setup, select any one among *Internet*, *Local intranet*, *Trusted sites* or *Restricted sites* and click **Custom level**. In the **Security Settings - <*option*> Zone** dialog box, under **Settings**, find **Downloads** option, enable **File download** option and click **OK** to the save the changes.
  For all other browsers, accept file download when prompted.
- **Enable JavaScript for this site** - Indicates whether the JavaScript setting is enabled in browser.
- **Enable cookies for this site** - Indicates whether the cookies setting is enabled in browser.
  Note: Cookies must be enabled to access the website.

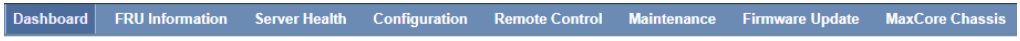
Downloaded from Arrow.com.

7.1.3 Using MegaRAC SP-X

The MegaRAC GUI consists of following menu tabs as shown below:

- Dashboard
- FRU Information
- Server Health
- Configuration
- Remote Control
- Maintenance
- Firmware Update
- MaxCore Chassis

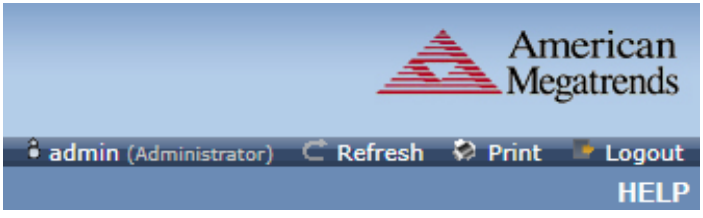
Figure 7-2 Menu Bar



7.1.3.1 Quick Button and Logged-in User

The user information and quick-action buttons are located at the top right of the MegaRAC GUI. A screen shot of the logged-in user information is shown below.

Figure 7-3 Logged-in User Information



The logged-in user information screen shows the logged-in user, user's privilege, and three quick-action buttons.

Downloaded from Arrow.com.

Table 7-2 Logged-in User Information

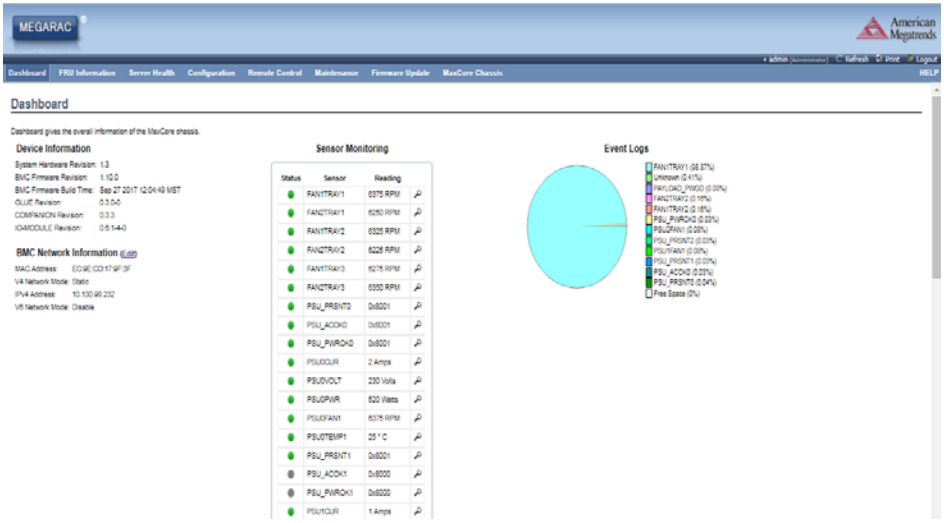
Command/Option Name	Description
<Username> (<Privilege>)	Shows the name of the logged-in user and assigned privileges. There are five types of users with their own privileges. ● **User**: Only valid commands are allowed. ● **Operator**: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces. ● **Administrator**: All BMC commands are allowed. ● **OEM Proprietary**: The user access level defined by OEM. ● **No Access**: Login access denied.
Refresh	Reloads the current page.
Print	Prints the current page.
Logout	Logs out the user from the application.
Help	Displays the application help page.

7.1.3.2 Dashboard

The **Dashboard** provides overall information about the status of a device. To open the **Dashboard**, click **Dashboard** tab from the menu bar.

Downloaded from Arrow.com.

Figure 7-4 Dashboard Screen



The following table contains **Dashboard** screen details.

Table 7-3 Dashboard

Field Name	Description
Device Information	Displays the Backplane Hardware Revision, the BMC Firmware Revision and Build Time (Date and Time). And the Backplane's GLUE, COMPANION, and IO-Module CPLD Revision.
BMC Network Information	Shows network settings for the device. Click **Edit** to modify the network information.
Sensor Monitoring	Lists all the available sensors on the device with the following information.
Status	Displays the state of the device. There are three states. ● - Denotes Normal state ● - Denotes Warning state ● - Denotes Critical state

Downloaded from Arrow.com.

Table 7-3 Dashboard (continued)

Field Name	Description
Sensor	States the name of the sensor.
Reading	Displays the value of sensor readings.
	Click this icon in-line with the respective sensor to display the sensor page for that particular sensor.
Event Logs	A graphical representation of all events incurred by various sensors and occupied/available space in logs can be viewed. If you click the color-coded rectangle in the Legend in the chart, you can view the list of those specific events only.

7.1.3.3 Field Replaceable Unit Information

FRU Information page displays the FRU device information of the Artesyn PCIE cards and PSUs. This page shows information like Basic Information, Chassis Information, Board Information, and Product Information of the FRU device.

Downloaded from Arrow.com.

To open the **FRU Information** page, click **FRU Information** tab on the menu bar.

Figure 7-5 FRU Information Page

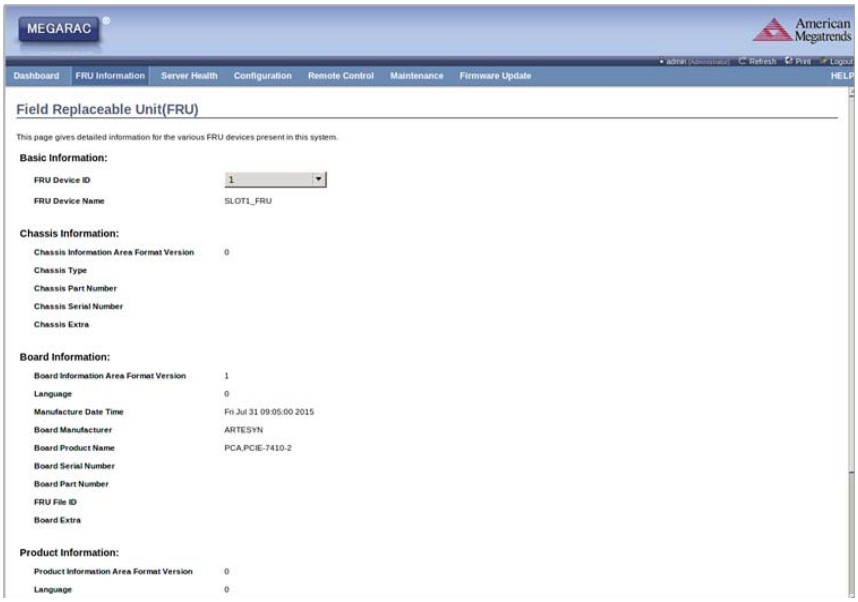


Table 7-4 FRU Information

Field Name	Description
Basic Information	Displays basic FRU information. Select the FRU device ID from the **FRU Device ID** drop-down list to view the details of respective FRU.
Chassis Information	Displays chassis information.
Board Information	Displays board information.
Product Information	Displays product information.
MAC address Record Information	Displays MAC address information.
PCIE Zone Record Information	Displays PCIE Zone Record information.

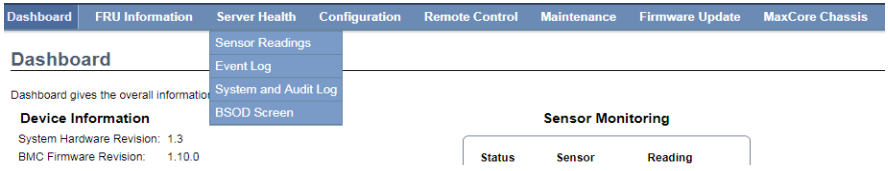
Downloaded from Arrow.com.

7.1.3.4 Server Health

The **Server Health** menu contains the following details:

- Sensor Readings
- Event Log
- System and Audit Log
- BSOD Screen

Figure 7-6 Server Health Menu

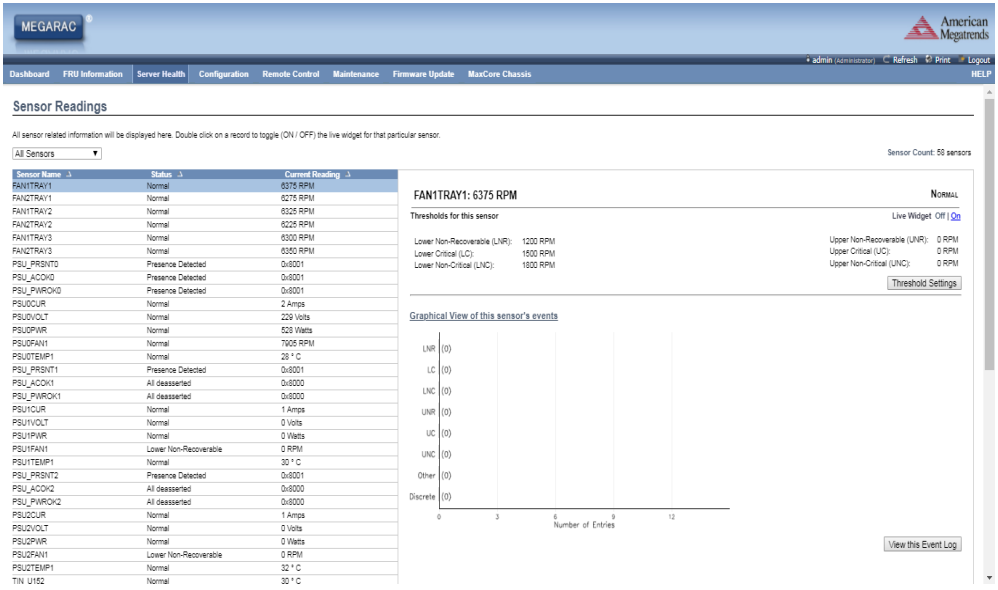


7.1.3.4.1 Sensor Readings

The **Sensor Readings** screen displays all the sensor related information. To open the **Sensor Readings** screen, clik **Server Health** > **Sensor Readings** from the menu.

Downloaded from Arrow.com.

Figure 7-7 Sensor Readings



Click on any sensor in the table to show more information about that particular sensor, including thresholds and a graphical representation of all associated events.

The **Sensor Readings** screen contains the following information.

You can choose the sensor type that you want to display from the drop-down box:

- All Sensors
- Temperature Sensors
- Voltage Sensors
- Current Sensors
- Fan Sensors
- Power Supply
- Cooling Device

Downloaded from Arrow.com.

If you select *All Sensors*, all the available sensors with details like Sensor Name, Status, and Current Reading will be appeared. Select a particular sensor from the list. On the right hand side of the screen you can view the thresholds of that sensor.

Thresholds are of six types:

- Lower Non-Recoverable (LNR)
- Lower Critical (LC)
- Lower Non-Critical (LNC)
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)

The threshold states could be *Lower Non-critical - going low*, *Lower Non-critical - going high*, *Lower Critical - going low*, *Lower Critical - going high*, *Lower Non-recoverable - going low*, *Lower Non-recoverable - going high*, *Upper Non-critical - going low*, *Upper Non-critical - going high*, *Upper Critical - going low*, *Upper Critical - going high*, *Upper Non-recoverable - going low*, and *Upper Non-recoverable - going high*.

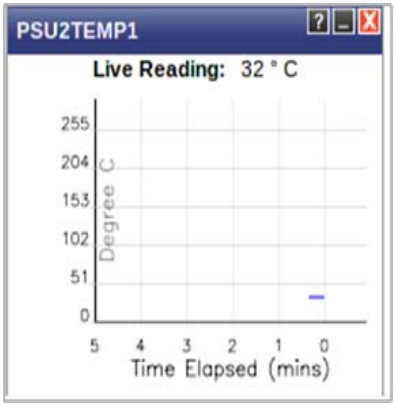
A graphical view of these events (Number of Entries vs. Thresholds) can be viewed as shown in the Figure 7-7.

Live Widget

For the selected sensor, you can click ON or OFF to turn the widget appear or disappear. This widget gives a dynamic representation of the readings for the sensor. You can also double click on a record to toggle (ON / OFF) the live widget for that particular sensor. Given below is a sample screen, when the widget is on.

Downloaded from Arrow.com.

Figure 7-8 Widget



Widgets are little gadgets, which provide real time information about a particular sensor. You can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget. The session will not expire, until the widgets get the live data of the last widget that is kept opened.

To view the Event Log for the selected sensor, click **View this Event Log** button.

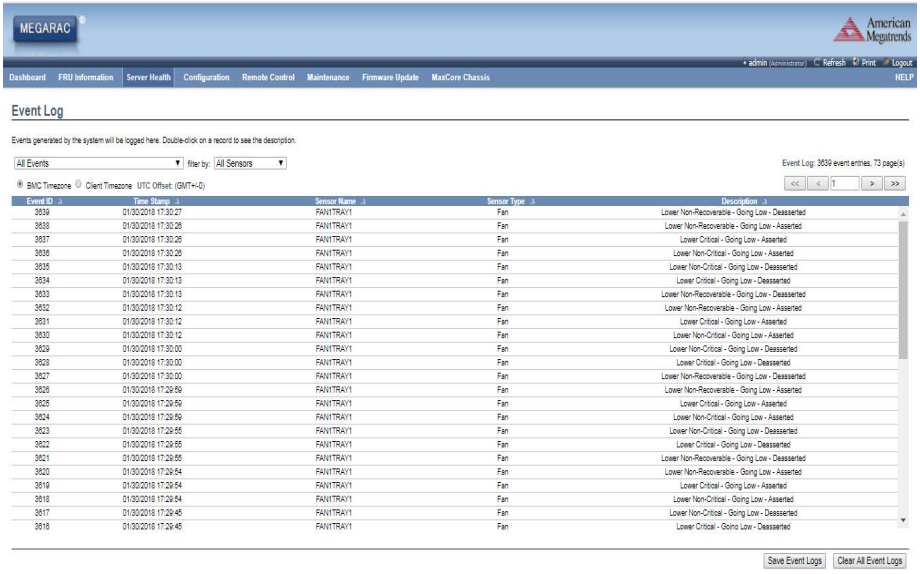
7.1.3.4.2 Event Log

The **Event Log** screen displays the list of event logs occurred by the different sensors on this device. Double-click on a record to see the details of that entry. You can use the sensor type or sensor name filter options to view those specific events or you can also sort the list of entries by clicking on any of the column headers.

Downloaded from Arrow.com.

To open the **Event Log** screen, click **Server Health** > **Event Log** from the menu bar. A sample view of **Event Log** screen is shown below.

Figure 7-9 Event Log



The following table contains the field and button description of the **Event Log** screen.

Table 7-5 Event Log

Field Name	Description
Event log Category	The category could be either *All Events*, *System Event Records*, *OEM Event Records*, *BIOS Generated Events*, *SMI Handler Events*, *System Management Software Events*, *System Software - OEM Events*, *Remote Console Software Events*, and *Terminal Mode Remote Console Software Events*.
Filter By	Filtering can be done with the sensors mentioned in the list. **Note**: Once the Event Log category and Filter type are selected, the list of events will be displayed with the Event ID, Time Stamp, Sensor Type, Sensor Name and Description.
BMC Timezone	Displays the events with BMC UTC Offset timestamp.

Downloaded from Arrow.com.

Table 7-5 Event Log (continued)

Field Name	Description
Client Timezone	Displays the events with Client UTC Offset timestamp.
UTC Offset	Displays the current UTC Offset value based on which event time stamps will be updated. Navigational arrows can be used to selectively access different pages of the Event Log.
Clear All Event Logs	To delete all the event logs.
Save Event Logs	To save all the existing event logs.

Procedure

To work on Event Logs, perform the following steps:

1. From the **Event Log Category** drop-down menu, select the event categories.
2. From the **Filter Type** drop-down list, select the sensor name to view the events for the selected filter.
3. Select either **BMC Timezone** or **Client Timezone**. The events will be displayed based on the selected time zone value.
4. To clear all events from the list, click **Clear All Event Logs** button.
5. To save all the existing event logs, click **Save Event Logs** button.

7.1.3.4.3 System and Audit Log

System and Audit Log screen will display all the system and audit events occurred against the device that has been already configured.



You have to configure logs under **Configuration** > **System and Audit Log** in order to display any entries.

To open the **System & Audit** Logs screen, click **Server Health** > **System and Audit Log** from the menu bar.

Downloaded from Arrow.com.

Figure 7-10 shows the **System & Audit Logs** screen view.

Figure 7-10 System and Audit Logs - System Log Tab

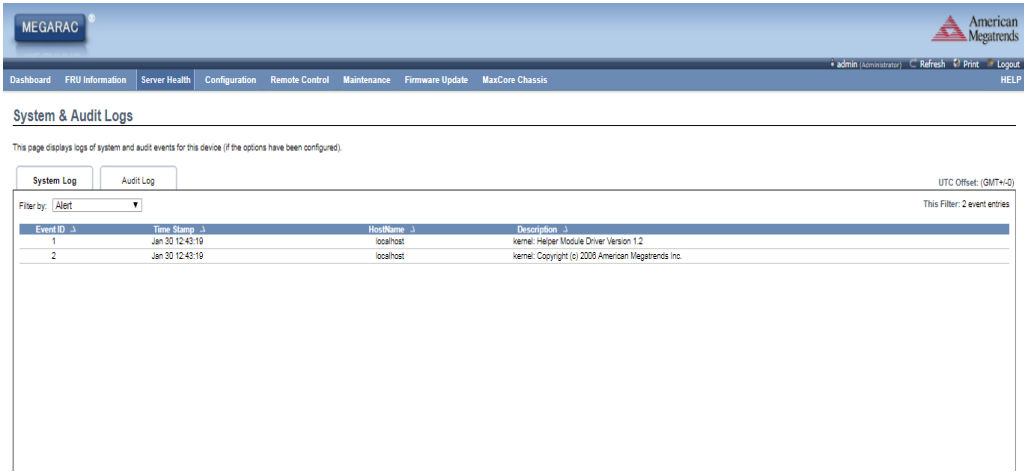
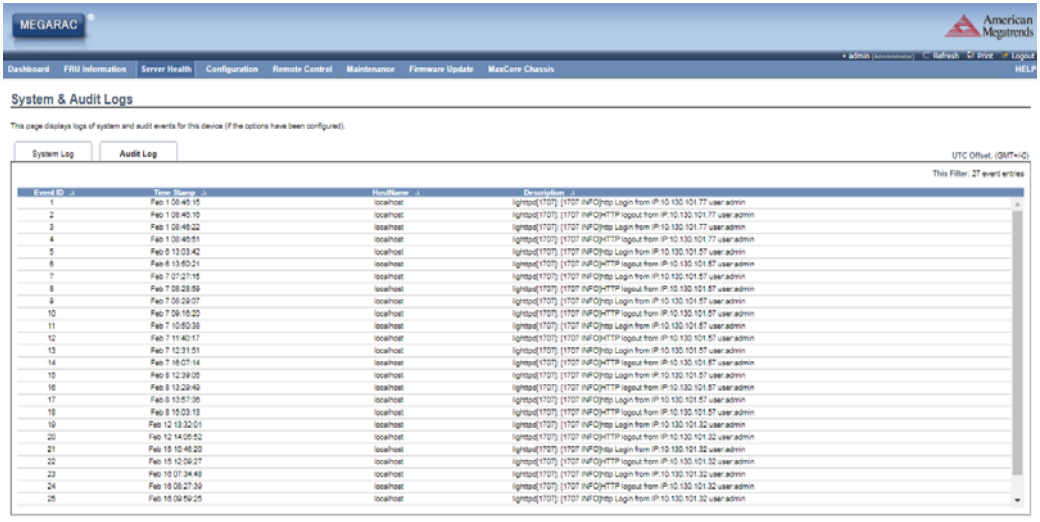


Figure 7-11 System and Audit Logs - Audit Log Tab



Downloaded from Arrow.com.

Procedure

To view System Log and Audit Logs details:

1. Click the **System Log** tab to view all system events. You can filter the entries based on *Alert*, *Critical*, *Error*, *Notification*, *Warning*, *Debug*, *Emergency*, and *Information* types.
2. Click the **Audit Log** tab to view all audit events for this device.

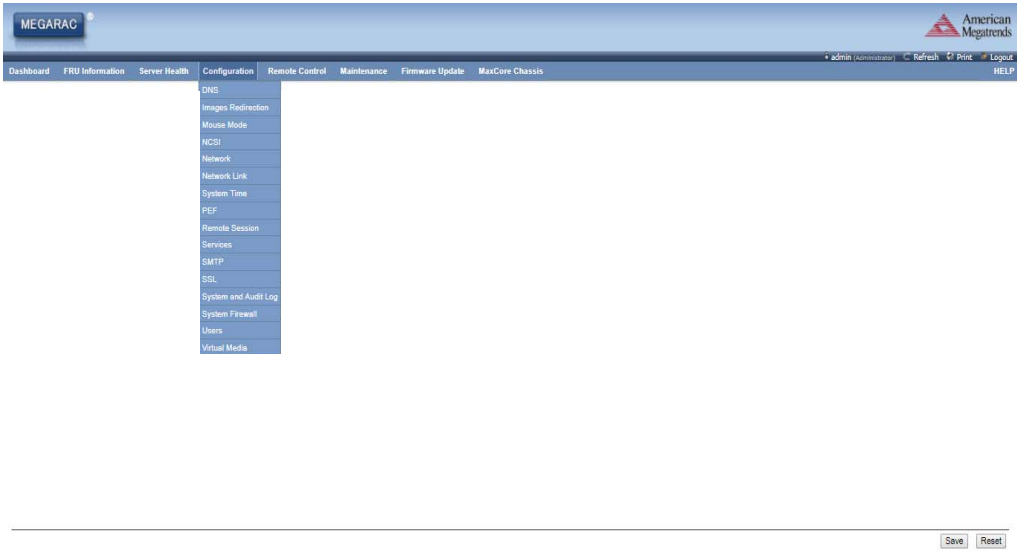
7.1.3.4.4 BSOD

TBD

7.1.3.5 Configuration Group

This group of pages allows you to access various configuration settings. Figure 7-12 shows the view of **Configuration** menu options.

Figure 7-12 Configuration Menu



Downloaded from Arrow.com.

A detailed description of the **Configuration** menu is given below.

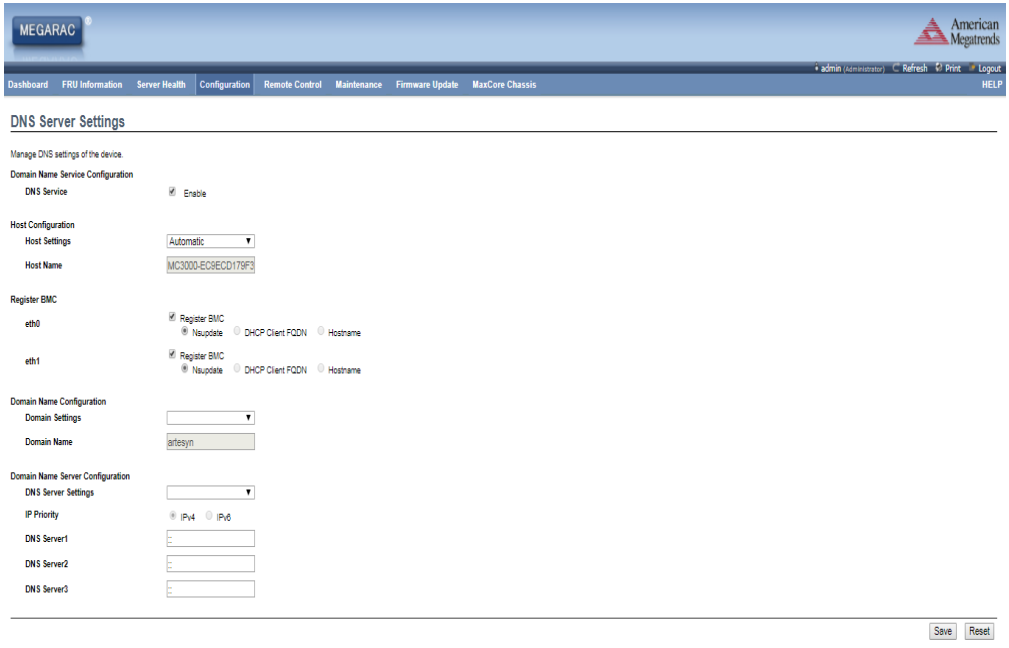
7.1.3.5.1 Domain Name System (DNS)

The Domain Name System (DNS) is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

The **DNS Server settings** screen is used to manage the DNS settings of a device.

To open **DNS Server Settings** screen, click **Configuration** > **DNS** from the menu bar. Figure 7-13 shows a sample view of **DNS Server Settings** screen.

Figure 7-13 DNS Server Settings



Downloaded from Arrow.com.

The following table contains the field and button description of **DNS Server Settings** screen.

Table 7-6 DNS Server Settings

Field Name	Description
Domain Name Service Configuration	
DNS Service	To enable/disable all the DNS Service Configurations.
Multicast DNS Support	
mDNS Settings	To enable/disable the mDNS Support Configurations.
Host Configuration	
Host Settings	Choose either Automatic or Manual settings.
Host Name	It displays host name of the device. If the Host setting is chosen as Manual, specify the host name of the device. **Note**: ● Value ranges from 1 to 64 alpha-numeric characters. ● Special characters '-'(hyphen) and '_'(underscore) are allowed. ● It must not start or end with a '-'(hyphen). IE browsers won't work correctly if any part of the host name contain underscore (_) character.
Register BMC	
Nsupdate	Maintenance utility
DHCP Client FQDN	DHCP client domain name
HostName	Name of the host
Domain Name Configuration	
Domain Settings	Lists the options for domain interface as Manual, *v4 or v6* for multiLAN channels. **Note**: If you choose DHCP, select v4 or v6 for DHCP servers.
Domain Name	Displays the domain name of the device. If the Domain setting is chosen as *Manual*, specify the domain name of the device. If you chose *Automatic*, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
Domain Name Server Configuration	

Downloaded from Arrow.com.

Table 7-6 DNS Server Settings (continued)

Field Name	Description
DNS Server Settings	Lists the option for v4 DNS settings for the device, Manual and available LAN interfaces.
IP Priority	• If IP Priority is IPv4, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server. • If IP Priority is IPv6, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server. **Note**: This is not applicable for Manual configuration.
DNS Server 1, 2 & 3	Specifies the DNS (Domain Name System) server address to be configured for the BMC. **Note**: • IPv4 Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". • Each number ranges from 0 to 255. • First number must not be 0. DNS Server Address will support the following: • IPv4 Address format • IPv6 Address format
Save	Saves the entered changes.
Reset	Clears the entered changes.

Procedure

To set DNS Server Settings, perform the following steps:

1. Under **Domain Name Service Configuration**, check the **Enable** option in-line with **DNS Service** to enable all the DNS Service Configurations.
2. Choose the **Host Configuration** either *Automatic* or *Manual*.
   Note: If you choose *Automatic*, you need not enter the Host Name and if you choose *Manual*, you need to enter the Host Name.
3. Enter the *Host Name* in the given field, if you have chosen *Manual* Configuration.

Downloaded from Arrow.com.

4. Under **Register BMC**, choose the BMC's network port to register with this DNS settings.
   - Check the option **Register BMC** to register with this DNS settings.
   - Choose the option **Direct Dynamic DNS** to register with direct dynamic DNS or choose **DHCP Client FQDN** to register through DHCP server.
5. Under the **Domain Name Configuration** pane:
   1. Select the required *Domain Settings* from the drop-down list.
   2. Enter the Domain Name in the given field, if the option *Manual* is being selected in **Domain Settings** field.
6. Under the **Domain Name Server Configuration** pane:
   1. Select the required *DNS Server Settings* from the drop-down list.
   2. Choose the IP Priority, either *IPv4* or *IPv6*.
   3. Enter the *DNS Server address*.
   4. In DNS Server1, DNS Server2 and DNS Server3, enter the server addresses to be configured for the BMC.
7. Click **Save** to save the entries.
8. Click **Reset** to clear the entries.

7.1.3.5.2 Images Redirection

Using **Image Redirection** screen, you can configure the images into BMC for redirection. This can be done either by uploading an image into BMC either from the Local Media or by mounting the image from the remote system, Remote Media.



In MC3000, the local media is limited by the memory or SPI flash size. The remote media is mounted (not uploaded) via network, and it supports Network File System (NFS) and Samba.

Downloaded from Arrow.com.

To open **Images Redirection** screen, click **Configuration** > **Images Redirection** from the menu bar. A sample view of **Images Redirection** screen is shown below.

Figure 7-14 Image Redirection



The following are tabs and key fields on the **Images Redirection** screen:

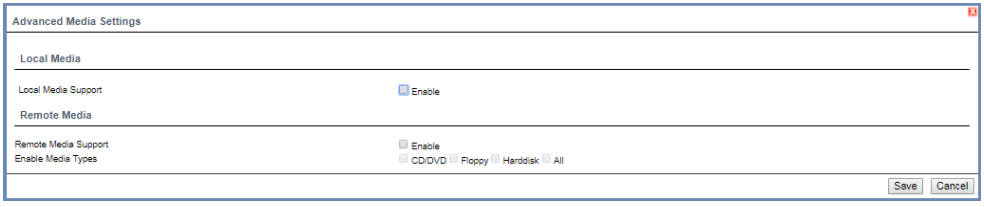
- Advanced Settings
- Local Media
- Remote Media

Advanced Settings

This option is used to configure Advanced Media Settings.

To open **Advanced Media Settings** screen, click **Configuration** > **Images Redirection** > **Advanced Settings**.

Figure 7-15 Advanced Media Settings



Downloaded from Arrow.com.

Table 7-7 Advanced Media Settings

Field Name	Description
Local Media	
Local Media Support	To enable or disable Local Media support, check/uncheck the 'Enable' check box.
Remote Media	
Remote Media Support	To enable or disable Remote Media support, check/uncheck the 'Enable' check box. **Note**: Both local and remote media support can be enabled at a time.
Enable Media Types	To edit any particular media type, select any one of the Remote Media Support from CDDVD, Floppy, Harddisk and All. You can also select all the media types simultaneously. **Note**: You can configure different settings for different remote media types by enabling corresponding media type.
Clear All Event Logs	Clears all the event logs.
Save Event Logs	Saves all the existing Event Log records.

Local Media

This tab displays the list of available images in the local media on BMC. You can replace or add new images from here. To configure the image, you need to enable **Local Media Support** under Figure "Advanced Media Settings" on page 138. Once you enable this option, the user can add the images and the added images will be redirected to the host machine.

Note:

- To replace or add an image, you must have Administrator Privileges.
- More than one image can be uploaded for each image type.
- In Local Media redirection, image upload size depends on SD card partition size. Totally 12 images can be redirected, if each partition of 4 images is configured for 3 media types.

Table 7-8 Local Media

Field Name	Description
Start/Stop Redirection	To start or stop Media redirection.

Downloaded from Arrow.com.

Table 7-8 Local Media (continued)

Field Name	Description
Add Image	To upload a new image to the device.
Delete Image	To delete the desired image.

Procedure

To configure local media settings, perform the followings steps:

1. To add or delete images, start/stop redirection and configure remote media images, click **Advanced Settings** and make sure **Local Media Support** option is enabled.
   Note: The Start Redirection button is active only for VMedia enabled users.
2. Click **Local Media** Tab.
3. Select a configured slot and click **Start Redirection** to start the local media redirection. A pop-up message will appear stating that the “Local Media Redirection is started”, click **OK** to continue. It is a toggle button, if the image is successfully redirected, click **Stop Redirection** to stop the local media redirection. A pop-up message will appear stating that the “Local Media Redirection is stopped”, click **OK** to continue.
4. To add an image, select a free slot and click **Add Image** to upload a new image to the device. A sample screen of **Add Image** dialog box is shown below.



5. To delete an image, select a record and click **Delete** Image to delete the selected image. A pop-up message will appear prompting you to continue, click **OK** to continue deleting the image.
   Note: Redirection needs to be stopped to delete the image.

Downloaded from Arrow.com.

Remote Media

The displayed table shows configured images on BMC. You can configure images of the remote media server.

Note:

- More than one image can be configured for each image type. At maximum 4 images can be configurable.
- To configure the image, You need to enable Remote Media support using 'Advanced Settings'.
- To start/stop redirection and to delete an image, you must have Administrator Privileges.
- Free slots are denoted by "~"

Table 7-9 Remote Media

Field Name	Description
Start/Stop Redirection	To start or stop Media redirection.
Clear Image	To clear the desired image.

Procedure

To configure remote media settings, perform the followings steps:

1. To **Start/Stop Redirection** and configure remote media images, click **Advanced Settings** and make sure **Remote Media Support** option is enabled.
   Note: The **Start Redirection** button is active only for VMedia enabled users.

2. Select a configured slot and click **Start Redirection** to start the remote media redirection. A pop-up message will appear stating that the "Local Media Redirection is stopped", click **OK** to continue.
   It is a toggle button, if the image is successfully redirected, click **Stop Redirection** to stop the remote media redirection. A pop-up message will appear stating that the "Local Media Redirection is stopped", click **OK** to continue.

Downloaded from Arrow.com.

3. To clear an image, click the configured slot, select an image to be deleted from the drop down box and click **Clear Image**. A pop-up message will appear prompting you to continue, click **OK** to continue clearing the image.
   Note: Redirection needs to be stopped to clear the image.

7.1.3.5.3 Mouse Mode

The Redirection Console handles mouse emulation from local window to remote screen using either of the three methods. Only 'Administrator' has the right to configure this option.

The following table provides fields and buttons on the **Mouse Mode Settings** screen.

Table 7-10 Mouse Mode Settings

Field Name	Description
Local Media	
Set Mode to Relative (Recommended when server OS is Linux)	The Relative mode sends the calculated relative mouse position displacement to the server. To select this mode select the "Set mode to Relative" option.
Set Mode to Absolute (Recommended when server OS is Windows)	The absolute position of the local mouse is sent to the server. To select this mode, select the "Set mode to Absolute" option. Recommended for Windows or latter Linux releases.
Set Mode to Other Mode (Recommended for SLES-11 OS Installation)	Select Other Mode to have the calculated displacement from the local mouse in the centre position, sent to the server. Use this mode for SLES 11 Linux OS installation.
Save	Saves the changes.
Reset	Reset the modified the changes.

7.1.3.5.4 Network Controller Sideband Interface (NCSI)

In MegaRAC GUI, the **NCSI Settings** screen is used to configure Network Controller Sideband Interface (NCSI) configuration settings.

Downloaded from Arrow.com.

To open **NCSI Settings** screen, click **Configuration** > **NCSI** from the menu bar. A sample view of **NCSI Settings** screen is shown below.

Figure 7-16 NCSI Settings



Table 7-11 NCSI

Element Name	Description
NCSI Interface	Lists the interface name in list box.
Channel Number	Lists the channel number of the selected interface.
Package ID	Lists the package id of the selected interface.
Save	To save the current changes.
Reset	To reset the modified changes.

Procedure

To configure the channel number and package ID information for the NCSI interface, perform the following steps:

1. Choose the particular *NCSI Interface* to which you need to configure NCSI settings.
2. Choose the *Channel Number* to be configured for the selected Interface name.
3. Choose the *Package ID* to be configured for the selected Interface name.
4. Click **Save** to save the current changes.
5. Click **Reset** to reset the modified changes.

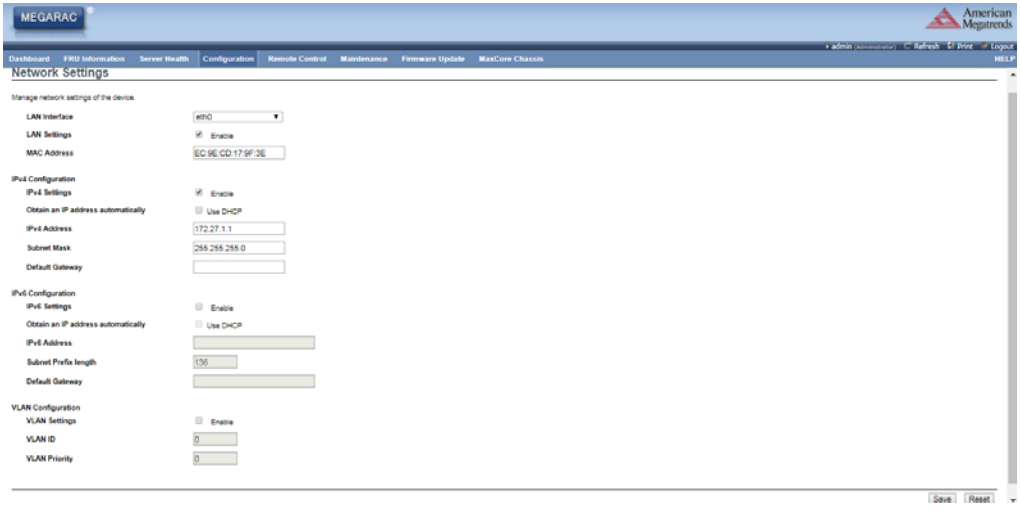
Downloaded from Arrow.com.

7.1.3.5.5 Network

In MegaRAC GUI, the **Network Settings** page is used to configure the network settings for the available LAN channels.

To open **Network Settings** page, click **Configuration** > **Network** from the menu bar. A sample view of **Network Settings** page is shown below.

Figure 7-17 Network Settings



The following table contains field and button description of **Network Settings** screen.

Table 7-12 Network Settings

Element Name	Description
LAN Interface	Lists the LAN interfaces.
LAN Settings	To enable or disable the LAN Settings.
MAC Address	Displays the MAC Address of the device. This is a read only field.
IPv4 Configuration	Lists the following IPv6 configuration settings.
IPv4 Settings	To enable/disable the IPv4 settings in the device.

Downloaded from Arrow.com.

Table 7-12 Network Settings (continued)

Element Name	Description
Obtain IP Address automatically	To dynamically configure IPv4 address using DHCP (Dynamic Host Configuration Protocol).
IPv4 Address, Subnet Mask, and Default Gateway	These fields are for specifying the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device. Note: ● IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". ● Each Number ranges from 0 to 255. ● First Number must not be 0.
IPv6 Configuration	Lists the following IPv6 configuration settings.
IPv6 Settings	This option is to enable/disable the IPv6 settings in the device.
Obtain an IPv6 address automatically	To dynamically configure IPv6 address using DHCP (Dynamic Host Configuration Protocol).
IPv6 Address	To specify a static IPv6 address to be configured to the device. For example,m2004::2010
Subnet Prefix length	To specify the subnet prefix length for the IPv6 settings. **Note**: Value ranges from 0 to 128.
Default Gateway	Specify v6 default gateway for the IPv6 settings. **Note**: If core feature IPV6_COMPLIANCE is enabled, the IPV6 default Gateway field will not be displayed.
VLAN Configuration	Lists the VLAN configuration settings.
VLAN Settings	To enable/disable the VLAN support for selected interface.
VLAN ID	The Identification for VLAN configuration. **Note**: Value ranges from 1 to 409.
VLAN Priority	The priority for VLAN configuration. Note: ● Value ranges from 1 to 7. ● 7 is the highest priority for VLAN.
Save	To save the entries.
Reset	To reset the modified changes.

Downloaded from Arrow.com.

Procedure

To manage network settings of the device, perform the following steps:

1. Select the **LAN Interface** from the drop down list.
2. Check **Enable** to enable the LAN Settings.
3. In IPv4 Configuration, enable **Use DHCP to Obtain an IP address automatically** to dynamically configure IPv4 address using DHCP.
4. If the field is disabled, enter the *IPv4 Address*, *Subnet Mask* and *Default Gateway* in the respective fields.
5. In IPv6 Configuration, if you wish to enable the IPv6 settings, check **Enable**.
6. If the IPv6 setting is enabled, enable or disable the option **Use DHCP for obtaining the IP address automatically**.
7. If the field is disabled, enter the *IPv6 Address*, *Subnet Prefix length* and *Default Gateway* in the given fields.
8. In VLAN Configuration, if you want to enable the VLAN settings, check *Enable*.
9. Enter the *VLAN ID* in the specified field.
10. Enter the *VLAN Priority* in the specified field.
11. Click **Save** to save the entries
12. Click **Reset** if you want to reset the modified changes.

7.1.3.5.6 Network Link

This page is used to configure the network link option for the available network interfaces.

To open **Network Link Configuration** page, click **Configuration** > **Network Link** from the menu bar.

Downloaded from Arrow.com.

The following table contains field and button description of **Network Settings** screen.

Table 7-13 Network Settings

Element Name	Description
LAN Interface	Select the network interface from the list for which the Link speed and duplex mode are to be configured.
Auto Negotiation	This option is enabled to allow the device to perform automatic configuration to achieve the best possible mode of operation (speed and duplex) over a link..
Link Speed	Link speed will list all the supported capabilities of the network interface. It can be 10/100/1000 Mbps. **Note**: Link speed of 1000 Mbps is not applicable, when Auto Negotiation is OFF.
Duplex Mode	Select any one of the following Duplex Modes. - Half Duplex - Full Duplex.
Save	To save the entries.
Reset	To reset the modified changes.

Procedure

To manage link settings of the device, perform the following steps:

1. Select the **LAN Interface** from the drop down list.
2. Select **Auto Negotiation** as either On or OFF.
3. Choose **Link Speed** and **Duplex Mode** from the respective drop-down lists.
4. Click **Save** to save the entries
5. Click **Reset** if you want to reset the modified changes.

7.1.3.5.7 System Time

MC3000 has a battery backed RTC to keep the time. The RTC time can be set manually or automatically updated from an NTP server.

Downloaded from Arrow.com.

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It is designed particularly to resist the effects of variable latency by using a jitter buffer.

In MegaRAC GUI, this page displays the device current date and time settings. It can be used to configure either Date & Time or NTP server settings for the device.

To open **NTP Settings** screen, click **Configuration** > **NTP** from the menu bar. A sample view of **NTP Settings** screen is shown below.

Figure 7-18 NTP Settings



The following table contains field and button description of **NTP Settings** screen.

Table 7-14 NTP Settings

Element Name	Description
Date	To specify the current date of the device
Time	To specify the current Time for the device. **Note**: As Year 2038 Problem exists, Date and Time should be configured within the range.
TimeZone	Timezone list contains the UTC offset along with the locations and Manual UTC offset for NTP server, which can be used to display the exact local time.
Primary NTP Server & Secondary NTP Server	NTP Server fields will support the following: ● IP Address (Both IPv4 and IPv6 format). ● FQDN (Fully qualified domain name) format. ● FQDN Value ranges from 1 to 128 alpha-numeric characters.

Downloaded from Arrow.com.

Table 7-14 NTP Settings (continued)

Element Name	Description
Automatically synchronize Date & Time with NTP Server	To automatically synchronize Date and Time with the NTP Server.
Refresh	To reload the current date and time settings.
Save	To save the entries.
Reset	To reset the modified changes.

Procedure

To configure the NTP server and modify the device Date and Time settings, perform the following steps:

1. Enter the Date and Time in the given fields.
   Note: These fields are enabled only when the option **Automatically synchronizes Date & Time with NTP Server** is disabled.
2. Select the *Timezone* from the drop-down list.
3. In the **Primary NTP Server / Secondary NTP Server** field, specify the NTP server for the device.
   Note: Secondary NTP server is optional field.If the Primary NTP server is not working fine, the Secondary NTP Server will be tried.
4. Enable the **Automatically synchronize Date & Time with NTP Server** option to automatically synchronize date and time with NTP Server.
5. Click **Refresh** button to reload the date and time settings.
6. Click **Save** button to save the entries.
7. Click **Reset** button to reset the entries.

7.1.3.5.7.1 Shelf-wide time Synchronization

shelfHost has direct access to the MC3000 BMC and its clock is synchronized with the MC3000 RTC. However, all other CPUs do not have such access. So, a mechanism needs to be implemented on these CPUs to keep the time in sync with the shelfHost CPU or the BMC.

Downloaded from Arrow.com.

7.1.3.5.8 Platform Event Filtering (PEF)

Platform Event Filtering (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.

In MegaRAC GUI, the PEF Management is used to configure the following:

- Event Filter
- Alert Policy
- LAN Destination

To open **PEF Management Settings** screen, click **Configurations** > **PEF** from the menu bar. Each tab is explained below.

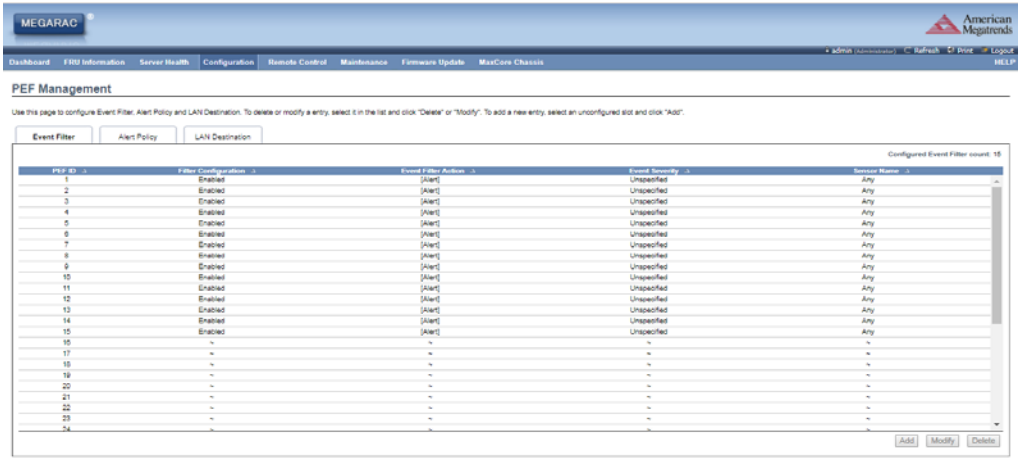
Event Filter Tab

A PEF implementation is recommended to provide at least 15 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, and so on. Remaining entries can be made available for 'OEM' or System Management Software configured events.

Downloaded from Arrow.com.

Note: The individual entries can be tagged as being reserved for system use. So, this ratio of pre-configured entries to run-time configurable entries can be re-allocated, if necessary.

Figure 7-19 PEF Management - Event Filter



The fields of **PEF Management** > **Event Filter** tab are explained below. This page contains a list of configured PEFs.

PEF ID: This field displays the ID for the newly configured PEF entry (read-only).

Filter Configuration: Check box to enable the PEF settings.

Event Filter Action: Check box to enable PEF Alert action. This is a mandatory field.

Event Severity: To choose any one of the Event severity from the list.

Sensor Name: To choose the particular sensor from the sensor list.

Add: To add the new event filter entry and return to Event filter list.

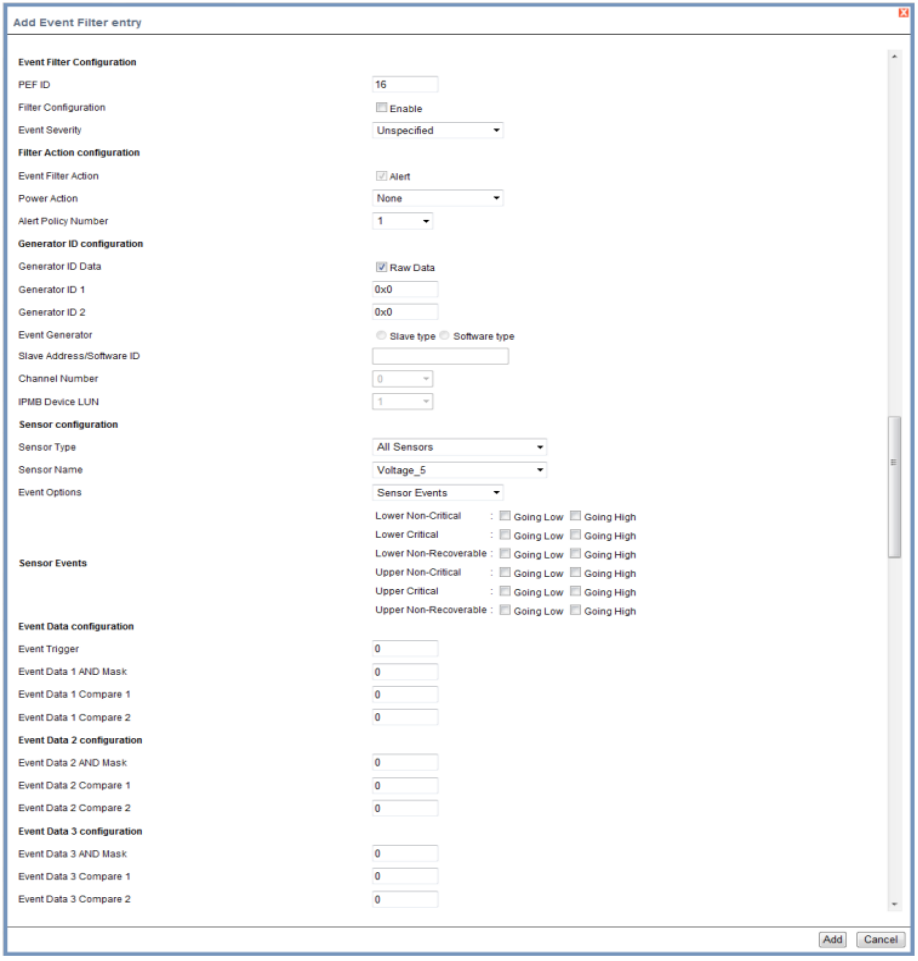
Modify: To modify the existing entries.

Delete: To delete the configured even filter.

Downloaded from Arrow.com.

Procedure:

1. Click the **Event Filter** tab to configure the event filters in the available slots.
2. To Add an Event Filter entry, select a free slot and click **Add** or alternatively double-click the empty slot to open the **Add Event Filter entry** page as shown below.



Downloaded from Arrow.com.

3. In the Event Filter Configuration section,
   a. **PEF ID** displays the ID for configured PEF entry (read-only).
   b. In **Filter Configuration,** check the box to enable the PEF settings.
   c. In **Event Severity,** select any one of the Event severity from the list.
4. In the Filter Action Configuration section,
   a. Event Filter Action is a mandatory field and checked by default, which enable PEF Alert action (read-only).
   b. Select any one of the Power Action either Power down, Power reset or Power cycle from the drop down list.
   c. Choose any one of the configured Alert Policy Number from the drop down list.



Alert Policy has to be configured under Configuration > PEF > Alert Policy.

5. In the Generator ID configuration section,
   a. Check Generator ID Data option to fill the Generator ID with raw data.
      – Generator ID 1 field is used to give raw generator ID1 data value.
      – Generator ID 2 field is used to give raw generator ID2 data value.



In RAW data field, specify hexadecimal value prefix with ‘0x’.

   b. In the **Event Generator** section, choose the event generator as Slave Address - if event was generated from IPMB.Otherwise as System Software ID - if event was generated from system software.
   c. In the **Slave Address/Software ID** field, specify corresponding I2C Slave Address or System Software ID.

Downloaded from Arrow.com.

d. Choose the particular Channel Number that event message was received over Or choose '0' if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.

e. Choose the corresponding IPMB Device LUN if event generated by IPMB.

6. In the **Sensor configuration** section,

   a. Select the sensor type of sensor that will trigger the event filter action.

   b. In the **Sensor Name** field, choose the particular sensor from the sensor list.

   c. Choose event option to be either All Events or Sensor Specific Events.

7. In the **Event Data configuration** section,
   Event Trigger field is used to give Event/Reading type value.
   Note: Value ranges from 1 to 255.

   a. **Event Data 1 AND Mask** field indicates wild-carded or compared bits.
   Note: Value ranges from 1 to 255.

   b. **Event Data 1 Compare** 1 and **Event Data 1 Compare 2** fields are used to indicate whether each bit position's comparison is an exact comparison or not.
   Note: Value ranges from 1 to 255.

8. In the **Event Data 2 Configuration** section,

   a. **Event Data 2 AND Mask** field is similar to Event Data 1 AND Mask.

   b. Event Data 2 Compare 1 & Event Data 2 Compare 2 fields are similar to Event Data 1 Com-pare 1 and Event Data 1 Compare 2 respectively.

9. In the **Event Data 3 Configuration** section,

   a. Event Data 3 AND Mask field is similar to Event Data 1 AND Mask.

   b. Event Data 3 Compare 1 & Event Data 3 Compare 2 fields are similar to Event Data 1 Com-pare 1 and Event Data 1 Compare 2 respectively.

10. Click **Add** to save the changes and return to event filter list.

11. Click on **Cancel** to cancel the modification and return to Event filter list.

12. In the Event filter list, select the configured slot and click **Modify** or alternatively double click the configured slot to modify the existing event filter entry.

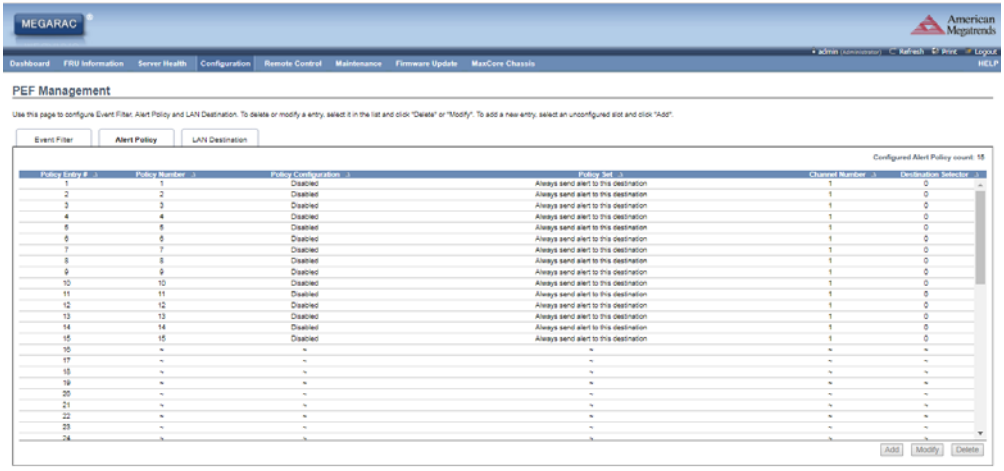
13. In the Event filter list, click **Delete** to delete the existing filter.

Downloaded from Arrow.com.

Alert Policy Tab

This screen is used to configure the Alert Policy for the PEF configuration. You can add, delete, or modify an entry in this screen.

Figure 7-20 PEF Management - Alert Policy



The fields of **PEF Management** > **Alert Policy** tab are explained below.

Policy Entry #: Displays Policy entry number for the newly configured entry (read-only).

Policy Number: Displays the Policy number of the configuration.

Policy Configuration: To enable or disable the policy settings.

Policy Set: To choose any one of the Policy Set values from the list.

0 - Always send alert to this destination.

1 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.

2 - If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set.

Downloaded from Arrow.com.

3 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.

4 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.

Channel Number: To choose a particular channel from the available channel list.

Destination Selector: To choose a particular destination from the configured destination list.

Note: LAN Destination has to be configured - under Configuration->PEF->LAN Destination.

Add: To save the new alert policy and return to Alert Policy list.

Modify: To modify the existing entries.

Delete: To delete the selected configured Alert Policy.

Procedure:

1. In the **Alert Policy** Tab, select the slot for which you have to configure the Alert policy. That is, In the **Event Filter Entry Page**, if you have chosen Alert Policy number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Select the slot and click **Add** or alternatively double-click on the empty slot to open the **Add Alert Policy Entry Page** as shown in the screen below.



Note: **Policy Entry #** is a read-only field.

3. Select the **Policy Number** from the list.
4. In the **Policy Configuration field**, check **Enable** if you wish to enable the policy settings.

Downloaded from Arrow.com.

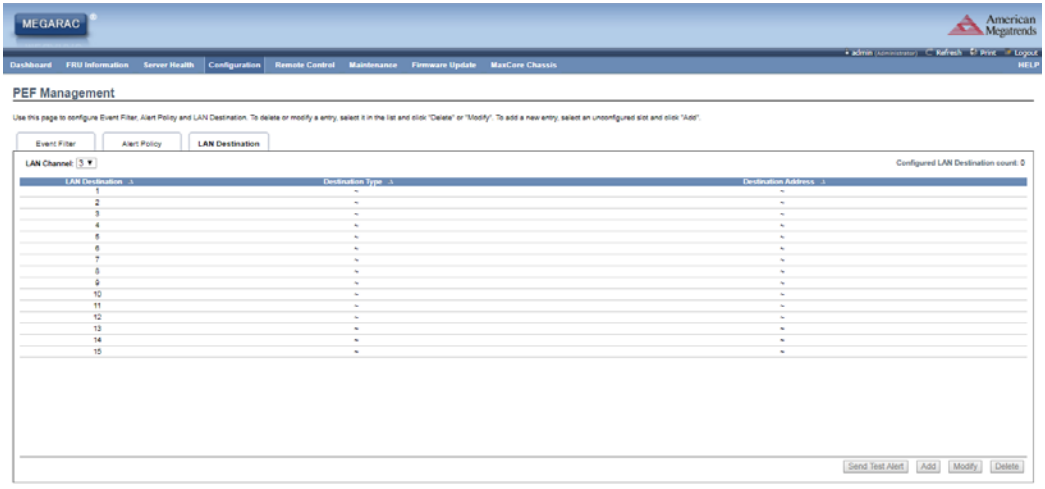
5. In the **Policy Set** field, choose any of the Policy set from the list.
6. In the **Channel Number field**, choose particular channel from the available channel list.
7. In the **Destination Selector field,** choose particular destination from the configured destination list.
   Note: LAN Destination has to be configured under Configuration->PEF->LAN Destination. That is if you select the number 4 for destination selector in Alert Policy Entry page, you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destination tab.
8. In the **Alert String** field, enable the check box if the Alert policy entry is Event Specific.
9. In the **Alert String Ke**y field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.
10. Click **Add** to save the new alert policy and return to Alert Policy list.
11. Click **Cancel** to cancel the modification and return to Alert Policy list.
12. In the Alert Policy list, to modify a configuration, select the slot to be modified and click **Modify** or alternatively double click on the configured slot that you wish to modify.
13. In the **Modify Alert Policy Entry Page**, make the necessary changes and click **Modify**.
14. In the Alert Policy list, to delete a configuration, select the slot and click **Delete**.

Downloaded from Arrow.com.

LAN Destination Tab

This screen is used to configure the LAN destination of PEF configuration. A sample view of **LAN Destination** screen is given below.

Figure 7-21 PEF Management LAN Destination



The fields of **PEF Management** > **LAN Destination** tab are explained below.

LAN Channel Number: Displays LAN Channel Number for the selected slot (read-only).

LAN Destination: Displays Destination number for the newly configured entry (read-only).

Destination Type: Destination type can be either an SNMP Trap or an E-mail alert. For E-mail alerts, the 3 fields - destination E-mail address, subject and body of the message needs to be filled.

The SMTP server information also has to be added - under Configuration->SMTP. For SNMP Trap, only the destination IP address has to be filled.

- IPv4 address format
- IPv6 address format

Downloaded from Arrow.com.

Subject & Message: These fields must be configured, if e-mail alert is chosen as destination type with the user configured in FixedSubject-Format. If the selected user for mail alert is configured with AMI-Format, the Subject and message fields will be grayed out. An e-mail will be sent to the configured e-mail address in case of any severity events with a subject specified in subject field and will contain the message field's content as the e-mail body.

Note: User should be configured under **Configuration > Users**.

Send Test Alert: To send sample alert to configured destination.

Note: Test alert can sent only with enabled SMTP configuration. SMTP support can be enabled under **Configuration > SMTP**.

Add: To add a new entry to the device. Alternatively, double click on a free slot.

Modify: To modify that entry. Alternatively, double click on the configured slot.

Delete: To delete the selected configured LAN Destination.

Procedure:

1. In the **LAN Destination Tab**, choose the slot to be configured. This should be the same slot that you have selected in the Alert Policy Entry- Destination Selector field. That is, if you have chosen the Destination Selector as 4 in the Alert Policy Entry page of **Alert Policy** Tab, you have to configure the 4th slot of LAN Destination Page.
2. Select the slot and click **Add** or alternatively double click on the empty slot. This opens the **Add LAN Destination entry**.



3. In the **LAN Channel Number** field, the LAN Channel Number for the selected slot is displayed and this is a read only field.

Downloaded from Arrow.com.

4. In the **LAN Destination** field**,** the destination for the newly configured entry is displayed and this is a read only field.
5. In the **Destination Type** field, select the one of the types.
6. In the **Destination Address** field, enter the destination address.
   Note: If Destination type is E-mail Alert, give the e-mail address that will receive the e-mail.
7. If the destination type is Email alert, select the User Name from the list of users.
   Note: E-mail address should be configured under **Configuration > Users**.
8. In the **Subject** field, enter the subject.
9. In the **Message** field, enter the message.
10. Click **Add** to save the new LAN destination and return to LAN destination list.
11. Click **Cancel** to cancel the modification and return to LAN destination list.
12. In the **LAN Destination** Tab, to modify a configuration, select the row to be modified and click **Modify** or alternatively double click the configured entry that you wish to modify.
13. In the **Modify LAN Destination Entry** page, make the necessary changes and click **Modify**.
14. In the **LAN Destination** Tab, to delete a configuration, select the slot and click **Delete**.

7.1.3.5.9 Remote Session

To open **Configure Remote Session** page, click **Configuration** > **Remote Session** from the menu bar.

The following table contains field and button description of **Remote Session** screen.

Table 7-15 Remote Session

Element Name	Description
Keyboard Languages	This select box is used to select the keyboard supported languages.
Virtual Media Attach Mode	Two types of VM attach modes are available: Attach - Immediately attaches Virtual Media to the server upon boot up. Auto Attach - Attaches Virtual Media to the server only when a virtual media session is started.

Downloaded from Arrow.com.

Table 7-15 Remote Session (continued)

Element Name	Description
Local Monitor OFF	Check this box to enable Local Monitor ON/OFF command can be enabled at runtime.
Automatically OFF Local Monitor, When JViewer Launches	Check this box to automatically Lock the local monitor, When JViewer launches.
Save	To save the entries.
Reset	To reset the modified changes.

Procedure

To manage link settings of the device, perform the following steps:

1. Select the **Keyboard Language** from the drop down list.
2. Select **Virtual Media Attach Mode** from the drop down list.
3. Select or clear **Local Monitor OFF** and **Automatically OFF Local Monitor** options.
4. Click **Save** to save the entries.
5. Click **Reset** if you want to reset the modified changes.

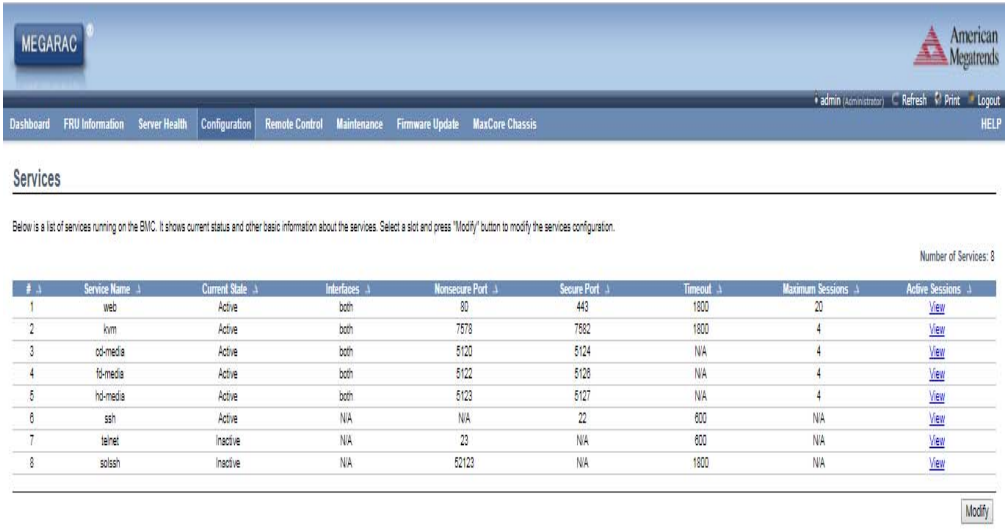
7.1.3.5.10 Services

This screen displays the basic information about services running in the BMC. Only Administrator can modify the service.

Downloaded from Arrow.com.

To open **Services** screen, click **Configuration** > **Services** from the menu bar. A sample view of **Services** page is shown below.

Figure 7-22 Services Page



The fields available on **Services** page are explained below.

Service Name: Displays service name of the selected slot (read-only).

Current State: Displays the current status of the service, either active or inactive state.

Interfaces: It shows the interface in which service is running.

Non-secure Port: This port is used to configure non secure port number for the service.

- Web default port is 80
- KVM default port is 7578
- CD Media default port is 5120
- FD Media default port is 5122
- HD Media default port is 5123
- Telnet default port is 23

Downloaded from Arrow.com.

Note: SSH service will not support non secure port. If single port feature is enabled, KVM, CD Media, FD Media and HD Media ports cannot be edited.

Secure Port: Used to configure secure port number for the service.

- Web default port is 443
- KVM default port is 7582
- CD Media default port is 5124
- FD Media default port is 5126
- HD Media default port is 5127
- SSH default port is 22

Note: Telnet service will not support secure port. If single port feature is enabled, KVM, CD Media, FD Media and HD Media ports cannot be edited.

Timeout: Displays the session timeout value of the service. For web, SSH and telnet service, user can configure the session timeout value.

- Web timeout value ranges from 300 to 1800 seconds.
- KVM timeout value ranges from 300 to 1800 seconds.
- SSH and Telnet timeout value ranges from 60 to 1800 seconds.
- SSH and telnet timeout value should be in multiples of 60 seconds.
- SSH and telnet service will be using the shared timeout value. If you configure SSH timeout value, it will be applied to telnet service also and vice versa.
- If KVM is launched, the web session timeout will not take effect.

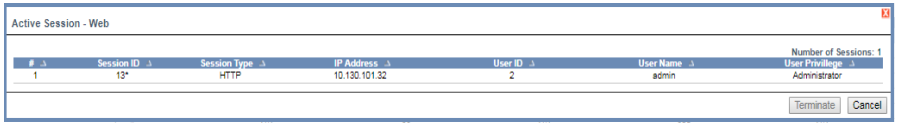
Maximum Sessions: Displays the maximum number of allowed sessions for the service.

Active Sessions: To view the current active sessions for the service.

Downloaded from Arrow.com.

Procedure

1. Click **View** to view the details about the active sessions for the service. This opens the **Active Session** dialog box (for example - Web Service screen), as shown in the screen below.



Session ID: Displays the ID number of the active sessions.
Session Type: Displays the type of the active sessions.
IP Address: Displays the IP addresses that are already configured for the active sessions.
User ID: Displays the ID number of the user.
User Name: Displays the name of the user.
User Privilege: Displays the access privilege of the user.

   a. Select a slot and click **Terminate** to terminate the particular session of the service else click **Cancel** to cancel the modification and return to Services list.

2. To modify the existing services.

   a. Select a slot and click **Modify** to modify the configuration of the service. Alternatively, double click on the slot. This opens the **Modify Service** dialog box as shown in the screen below.
   Note: Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.



Downloaded from Arrow.com.

Note: **Service Name** is a read-only field.

b. Activate the **Current State** by enabling the Activate check box.
Note: Interfaces, Non secure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.

c. Choose any one of the available interfaces from the **Interface** drop-down list.

d. Enter the Non secure port number in the **Non secure Port** field.

e. Enter the Secure Port Number in the **Secure Port** field.

f. Enter the timeout value in the **Timeout** field.
Note: The values in the **Maximum Sessions** field cannot be modified.

g. Click **Modify** to save the entered changes and return to the **Services** page else click **Cancel** to exit.

7.1.3.5.11 Simple Mail Transfer Protocol

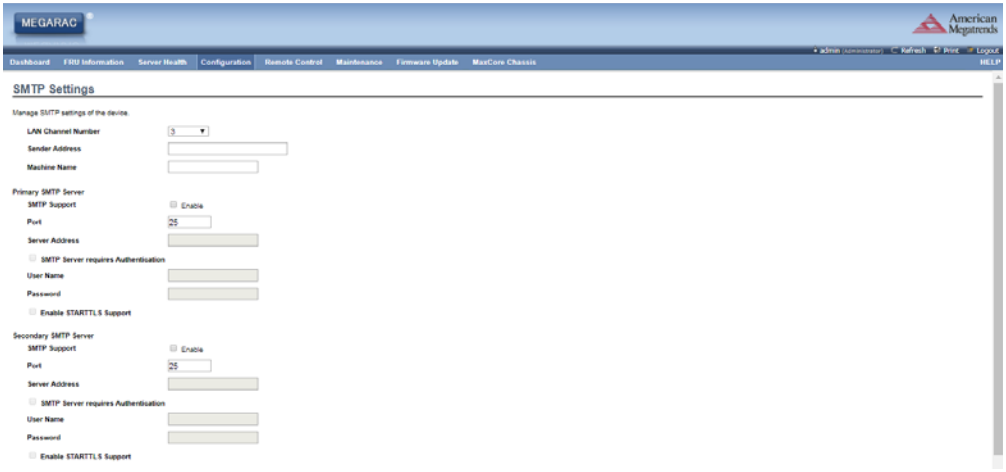
The Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across IP networks.

Using MegaRAC GUI, you can configure the SMTP settings of the device.

Downloaded from Arrow.com.

To open **SMTP Settings** screen, click **Configuration** > **SMTP** from the menu bar. A sample view of **SMTP Settings** screen is shown below.

Figure 7-23 SMTP Settings



The following table contains field and button description of **SMTP Settings** screen.

Table 7-16 SMTP Settings

Field Name	Description
LAN Channel Number	Displays the list of LAN channels available.
Sender Address	A valid 'Sender Address' to indicate the BMC, whenever e-mail is sent.
Machine Name	The 'Machine Name' of the BMC, from where the e-mail is sent. **Note**: ● Machine Name is a string of maximum 15 alpha-numeric characters. ● Space, special characters are not allowed.
Primary SMTP Server	Lists the Primary SMTP Server configuration.
SMTP Support	To enable/disable SMTP support for the BMC.

Downloaded from Arrow.com.

Table 7-16 SMTP Settings (continued)

Field Name	Description
Port	To specify the SMTP Port. **Note**: ● Default Port is 25. ● Port value ranges from 1 to 65535.
Server Address	The IP address of the SMTP Server. It is a mandatory field. **Note**: ● IP Address made of 4 numbers separated by dots as in "xxx.xxx. xxx.xxx". ● Each Number ranges from 0 to 255. ● First Number must not be 0. ● Supports IPv4 Address format and IPv6 Address format.
SMTP Server requires Authentication	To enable/disable SMTP Authentication. **Note**: The following are type of SMTP Server Authentication supported: ● CRAM-MD5 ● LOGIN ● PLAIN If the SMTP server does not support any one of the above authentication types, the user will get an error message stating, *Authentication type is not supported by SMTP Server.*
Username	Enter username to access SMTP Accounts. **Note**: ● User Name can be of length 4 to 64 alpha-numeric characters, dot(.), dash(-), and underline(_). ● It must start with an alphabet. ● Other Special Characters are not allowed.
Password	Enter password for the SMTP User Account. **Note**: ● Password must be at least 4 characters long. ● White space is not allowed. ● This field will not allow more than 64 characters.

Downloaded from Arrow.com.

Table 7-16 SMTP Settings (continued)

Field Name	Description
Enable STARTTLS Support	Check this option to enable STARTTLS support for the SMTP Client. **Note**: To enable STARTTLS support, the respective SMTP support option should be enabled.
SMTP CA Certificate File	File that contains the certificate of the trusted CA certs.
SMTP Certificate File	Client certificate filename.
SMTP Private Key	Client private key filename.
Secondary SMTP Server	Lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working fine, the device tries with the Secondary SMTP Server configuration.
Save	To save the entries.
Reset	To reset the modified changes.

Procedure

To manage SMTP settings of the device, perform the following steps:

1. Select the **LAN Channel Number** from the drop-down list.
2. Enter the *Sender Address* in the specified field.
3. Enter the *Machine Name* in the specified field.
4. Under **Primary SMTP Server**, select **Enable** check box to enable the **SMTP Support** option.
   Note: The Server Address can be edited only when the **SMTP Support** option is enabled.
5. Enter the *Port value* in the specified field.
6. Enter the *Server Address* in the specified field.
7. Select **SMTP Server requires Authentication** checkbox, if you want to authenticate SMTP Server.

Downloaded from Arrow.com.

8. Enter your *Username* and *Password* in the respective fields.
9. Under **Secondary SMTP Server**, select **Enable** checkbox to enable the **SMTP Support** option.
   Note: The Server Address can be edited only when the **SMTP Support** option is enabled. It is an optional field. If the Primary SMTP server is not working fine, the device tries with the Secondary SMTP Server configuration.
10. Enter the *Port value* in the specified field.
11. Enter the *Server Address* in the specific field.
12. Select **SMTP Server requires Authentication** checkbox, if you want to authenticate SMTP Server.
13. Enter your *Username* and *Password* in the respective field.
14. Click **Save** to save the entered details or click **Reset** to discard the entered details.

7.1.3.5.12 Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) protocol ensures secure transactions between web servers and browsers. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions.

Using MegaRAC GUI, configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open **SSL Certificate Configuration** page, click **Configuration** > **SSL** from the menu bar. There are three tabs on this page.

- **Upload SSL** option is used to upload the certificate and private key file into the BMC.
- **Generate SSL** option is used to generate the SSL certificate based on configuration details.
- **View SSL** option is used to view the uploaded SSL certificate in readable format.

Downloaded from Arrow.com.

A sample view of **SSL Certificate Configuration** (**Upload SSL** Tab) page is shown below.

Figure 7-24 SSL Certificate Configuration



The following table contains field and button description of **Upload SSL** tab screen.

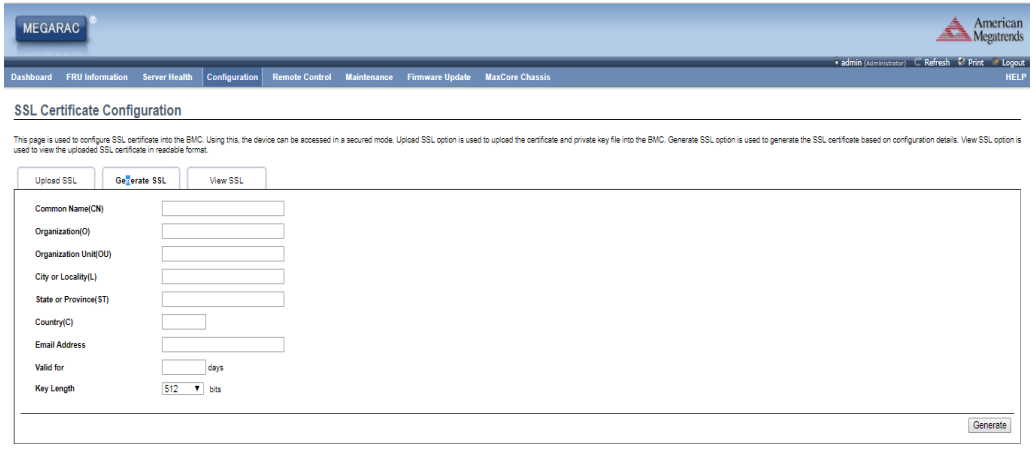
Table 7-17 Upload SSL

Field Name	Description
Current Certificate	Current certificate information will be displayed (read-only).
New Certificate	Certificate file should be of pem type.
Current Privacy Key	Current privacy key information will be displayed (read-only).
New Privacy Key	Privacy key file should be of pem type.
Upload	To upload the SSL certificate and privacy key into the BMC. **Note**: Upon successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.

Downloaded from Arrow.com.

A sample view of **Generate SSL** tab screen view is shown below.

Figure 7-25 SSL Certificate Configuration - Generate SSL



The following table contains field and button description of **Generate SSL** tab screen.

Table 7-18 Generate SSL

Field Name	Description
Common Name (CN)	Common name for which certificate is to be generated. ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
Organization (O)	Organization name for which the certificate is to be generated. ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
Organization Unit (OU)	Over all organization section unit name for which certificate is to be generated. ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
City or Locality (L)	City or Locality of the organization (mandatory). ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.

Downloaded from Arrow.com.

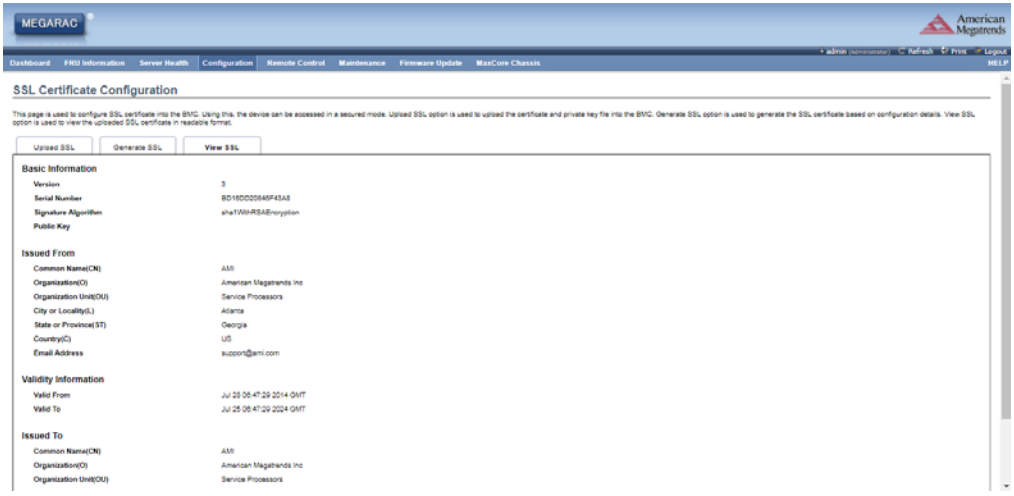
Table 7-18 Generate SSL (continued)

Field Name	Description
State or Province (ST)	State or Province of the organization (mandatory). ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
Country	Country code of the organization (mandatory). ● Only two characters are allowed. ● Special characters are not allowed.
Email Address	E-mail Address of the organization (mandatory).
Valid for	Validity of the certificate. Value ranges from 1 to 3650 days.
Key Length	The key length bit value of the certificate.
Generate	To generate the new SSL certificate.

Note: HTTPs service will get restarted, to use the newly generated SSL certificate.

A sample view of **View SSL** tab screen view is shown below.

Figure 7-26 SSL Certificate Configuration - View SSL



Downloaded from Arrow.com.

The following table contains field and button description of **View SSL** tab screen.

Table 7-19 Generate SSL

Field Name	Description
Common Name (CN)	Common name for which certificate is to be generated. ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
Organization (O)	Organization name for which the certificate is to be generated. ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
Organization Unit (OU)	Over all organization section unit name for which certificate is to be generated. ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
City or Locality (L)	City or Locality of the organization (mandatory). ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
State or Province (ST)	State or Province of the organization (mandatory). ● Maximum length of 64 characters. ● Special characters '#' and '$' are not allowed.
Country	Country code of the organization (mandatory). ● Only two characters are allowed. ● Special characters are not allowed.
Email Address	E-mail Address of the organization (mandatory).
Valid for	Validity of the certificate. Value ranges from 1 to 3650 days.
Key Length	The key length bit value of the certificate.
Generate	To generate the new SSL certificate.

Downloaded from Arrow.com.

Procedure

To configure SSL certificate into BMC, perform the following steps:

1. Click the **Upload SSL** Tab and browse the *New Certificate* and *New Privacy key*.
2. Click **Upload** to upload the new certificate and privacy key.
3. In **Generate SSL** tab, enter the required details.
4. Choose the *Key Length bit value* of the certificate.
5. Click **Generate** to generate the certificate.
6. Click **View SSL** tab to view the uploaded SSL certificate in user readable format.

Important points:

- Once you Upload/Generate the certificates, only HTTPs service will get restarted.
- You can now access your Generic MegaRAC® SP securely using the following format in your IP Address field from your Internet browser: *https://<your MegaRAC® SP's IP address here>*
- For example, if your MegaRAC® SP's IP address is 192.168.201.9, enter the following: *https://192.168.201.9*
- Note that the <s> after <http>.You must accept the certificate before you are able to access your Generic MegaRAC® SP.

7.1.3.5.13 System and Audit Log

In MegaRAC GUI, **System and Audit Log Settings** screen displays a list of system logs and audit logs occurred in this device.

Downloaded from Arrow.com.

To open **System and Audit Log Settings** screen, click **Configuration** > **System and Audit Log** from the menu bar. A sample view of **System and Audit Log Settings** page is shown below.

Figure 7-27 System and Audit Settings



The following table contains field and button description of **System and Audit Log Settings** screen.

Table 7-20 System and Audit Log Settings

Field Name	Description
System Log	To enable or disable the system logs.
Log Type	To Specify the Log type for system logs, whether it should be preserved in a local file or on a remote server. Note: Local file resides at /var/log/
File Size	To specify the size of the file in bytes if the selected log type is local. Note: Size ranges from 3 to 65535.
Rotate Count	To back up the log information in back up files. Note: ● Value ranges from 0 to 255. ● When log information exceeds the file size, the old log information is automatically moved to back up files based on the rotate count value. If rotate count is zero, old log information gets cleared permanently.

Downloaded from Arrow.com.

Table 7-20 System and Audit Log Settings (continued)

Field Name	Description
Server Address	This field is to specify the remote server address to log the system events. Note: Server address will support the following: ● IPv4 address format. ● FQDN (Fully qualified domain name) format.
Audit Log	To enable or disable the audit log.
Save	To save the configured settings.
Reset	To reset the previously saved values.

Procedure

To enable or disable logging of system or audit log events, perform the following steps:

1. In the **System Log** field, enable or disable the option.
2. Select the *Log Type*: *Local Log* or *Remote Log*.
3. If **Local Log i**s selected, enter the file size in the **File Size** field and rotate count in the **Rotate Count** field.
   Note: If **Remote Log** is selected, the fields *file size* and *rotate count* need not be mentioned.
4. If **Remote Log** is selected specify the *Server Address* of the remote server, where the system events are logged.
5. In the **Audit Log** field, check or uncheck the **Enable** option (as required).
6. Click **Save** to save the changes.
7. Click **Reset** to reset the entries.

Procedure

To configure the remote server to enable syslogging, perform the following steps:

Note: This example uses FC13 as the remote machine to log *syslog*.

Downloaded from Arrow.com.

On FC machine, disable the following lines for UDP in */etc/rsyslog.conf*.

- MODLOAD imudp
- UDPSERVER 514

7.1.3.5.14 System Firewall

In MegaRAC GUI, the **System Firewall** screen allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this screen, you must at least be an operator. Only administrators can add or delete a firewall.

To open **System Firewall** screen, click **Configuration** > **System Firewall** from the menu bar.

Figure 7-28 System Firewall



Procedure

To delete the settings:

1. Select the configured slot to be deleted and click **Delete**.

Procedure

To block or allow an IP address or range of IP addresses:

1. Click **Add** to add a new IP or range of IP address.

7.1.3.5.15 User Management

In MegaRAC GUI, the User Management page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

Downloaded from Arrow.com.

To open **User Management** screen, click **Configuration** > **Users** from the menu bar. A sample view of **User Management** screen is shown below. For security reasons, we strongly recommend you to change or remove the default user settings.

Figure 7-29 User Management

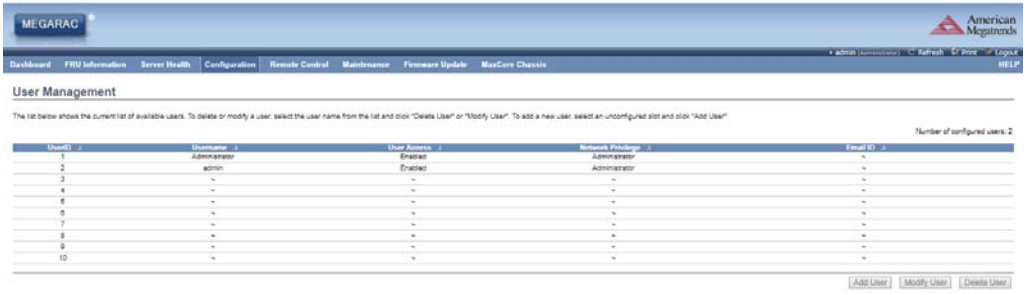


Table 7-21 User Management

Field Name	Description
User ID	Displays the ID number of the user. **Note**: The list contains a maximum of ten users only.
User Name	Displays the name of the user.
User Access	To enable or disable the access privilege of the user.
Network Privilege	Displays the network access privilege of the user.
SNMP Status	Displays if the SNMP status for the user is enabled or Disabled.
E-mail ID	Displays e-mail address of the user.
Add User	To add a new user.
Modify User	To modify an existing user.
Delete User	To delete an existing user.

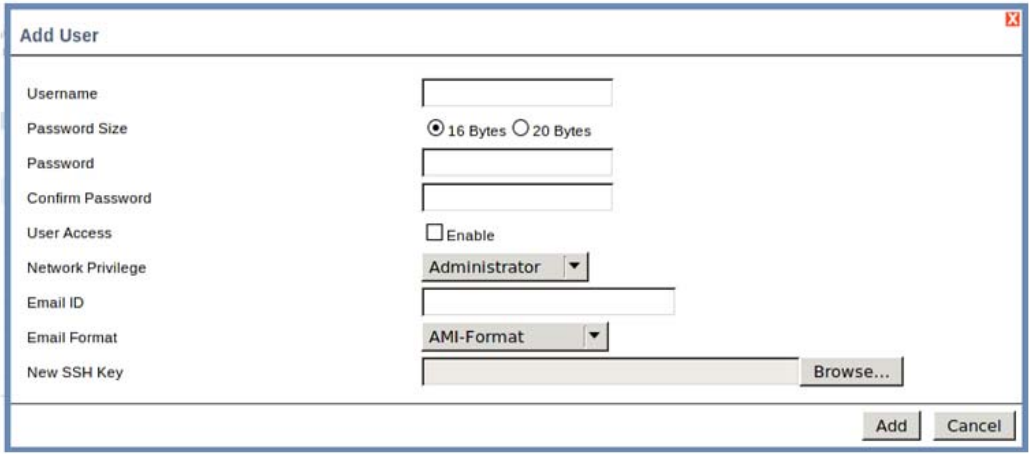
Procedure (Add User)

Note: The Free slots are denoted by "~" in all columns for the slot.

Downloaded from Arrow.com.

To add a new user, perform the following steps:

1. To add a new user, select a free slot and click **Add User** or alternatively double-click on the empty slot. This opens the **Add User** screen as shown below.



2. Enter the name of the user in the **Username** field.
   Note:
   - User Name is a string of 4 to 16 alpha-numeric characters.
   - It must start with an alphabetical character.
   - It is case-sensitive.
   - Special characters ‘,’(comma), ‘.’(period), ‘:’(colon), ‘;’(semicolon), ‘ ‘(space), ‘/’(slash), ‘\’(backslash), ‘(‘(left bracket) and ‘)’(right bracket) are not allowed.
3. In the **Password** and **Confirm Password** fields, enter and confirm your new password.
   Note:
   - Password must be at least 8 characters long.
   - White space is not allowed.
   - This field will not allow more than 20 characters.

Downloaded from Arrow.com.

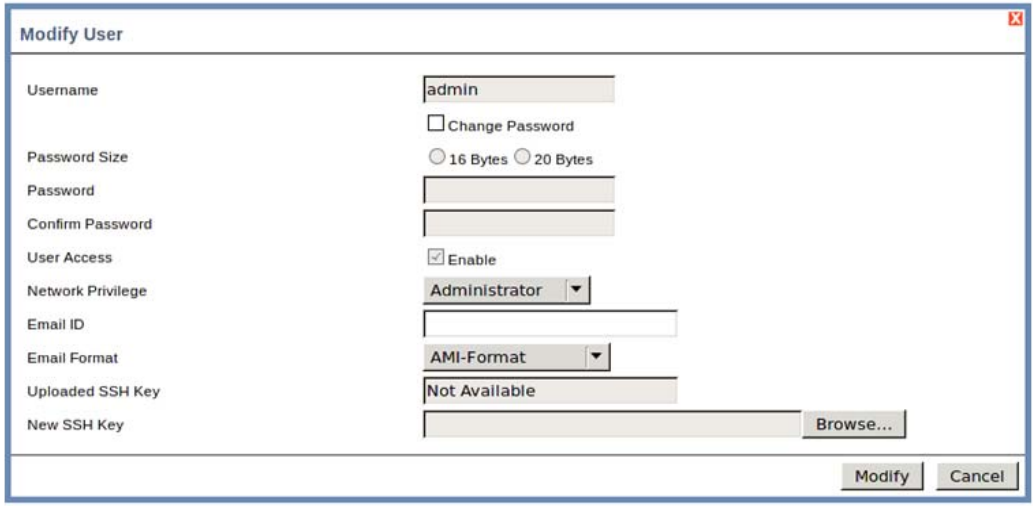
4. Enable or Disable the User Access Privilege.
5. In the **Network Privilege** field, enter the network privilege assigned to the user which could be Administrator, Operator, User or No Access.
6. In the **Email ID** field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.
   Note: SMTP Server must be configured to send emails.
   Email Format: Two types of formats are available:
   - **AMI-Format**: The subject of this mail format is 'Alert from (your Host name)'. The mail content shows sensor information, ex: Sensor type and Description.
   - **Fixed-Subject Format**: This format displays the message according to user's setting. You must set the subject and message for email alert.
7. In the **New SSH Key** field, click **Browse** and select the SSH key file.
   Note: SSH key file should be of pub type.
8. Click **Add** to save the new user and return to the users list.
9. Click **Cancel** to cancel the modification and return to the users list.

Downloaded from Arrow.com.

Procedure (Modify an Existing User)

To modify a user, perform the following steps:

1. Select an existing user from the list and click **Modify User** or alternatively double click on the configured slot. This opens the **Modify User** screen as shown below.



2. Modify the required field and click **Modify**.

Procedure (Delete User)

To delete an existing user, perform the following steps:

1. To delete an existing user, select the user from the list and click **Delete User**.
   Note: Reserved Users: There are certain reserved users which cannot be added as BMC Users. The list of reserved users is given below:
   - sysadmin
   - daemon
   - sshd

Downloaded from Arrow.com.

- ntp
- stunnel4

7.1.3.5.16 Virtual Media Devices

In MegaRAC GUI, this page is to configure Virtual Media Device settings. If you change the configuration of the virtual media in this page, it will show the appropriate devices in the JViewer VMedia Wizard. For example, if you select two floppy devices in **Configure** > **Virtual Media** screen, in **Jviewer** > **VMedia Wizard**, you can view two floppy devices available for redirection.

To open **Virtual Media** screen, click **Configuration** > **Virtual Media** from the menu bar. A sample view of **Virtual Media** screen is shown below.

Figure 7-30 Virtual Media



The following table contains field and button description of **Virtual Media** screen.

Table 7-22 Virtual Media

Field Name	Description
Floppy devices	The number of floppy devices supported for Virtual Media redirection.
CD/DVD devices	The number of CD/DVD devices supported for Virtual Media redirection.
Harddisk devices	The number of harddisk devices supported for Virtual Media redirection.
SD Media support	To Enable/Disable SD Media support in BMC.

Downloaded from Arrow.com.

Table 7-22 Virtual Media (continued)

Field Name	Description
Media Encryption	To Enable/Disable Encryption of Media data for the next redirection session. If Media Encryption is enabled, each CD,FD and HD media sessions will use their specific Secure ports which have been configured in Configuration > Services Page. **Note**: This option is disabled if Single Port is enabled in **Configuration** > **Remote Session** page

Procedure

To configure virtual media devices, perform the following steps:

1. Select the number of Floppy devices, CD/DVD devices, Harddisk devices from the respective drop-down list.
   Note: Maximum of two devices can be added in Floppy, CD/DVD and Harddisk drives.
2. Check the **SD Media support** option to enable/disable the SD card support in the host.
3. Check the **Media Encryption** option to enable/disable the Media Encryption data in the host.
4. Click **Save** to save the changes made or click **Reset** to reset the previously saved values.
   Note: If there are two device panels for each device, and when you click the **Connect** button, then the redirected device panel will be disabled.
   Unmounting device will make the driver disconnect device when using Auto Attach. Hence, when unmounting one USB key, the other USB key will be disconnected and then reconnected.
5. Click **Refresh** button to reload the date and time settings.
6. Click **Save** to save the entries or **Reset** button to reset the entries.

Downloaded from Arrow.com.

7.1.3.6 Remote Control

The **Remote Control** menu consists of Console Redirection and Chassis Power & Reset options.

7.1.3.6.1 Console Redirection

This screen allows you to view and control the power of your server. To open **Console Redirection screen**, click **Remote Control** > **Console Redirection** from the menu bar.

Figure 7-31 shows **Console Redirection** screen.

Figure 7-31 Console Redirection



Procedure

Click **VGA Console** button to launch the remote console redirection window from this page. To launch it, you must have Administrator privilege or KVM privilege.

By clicking the **VGA Console** button the jviewer.jnlp file will be downloaded. Once the file is downloaded and launched, a VGA redirection window will be displayed.

Note: A compatible JRE must be installed in the system prior to the launch of JNLP file.

7.1.3.6.2 Chassis Power Control and Status

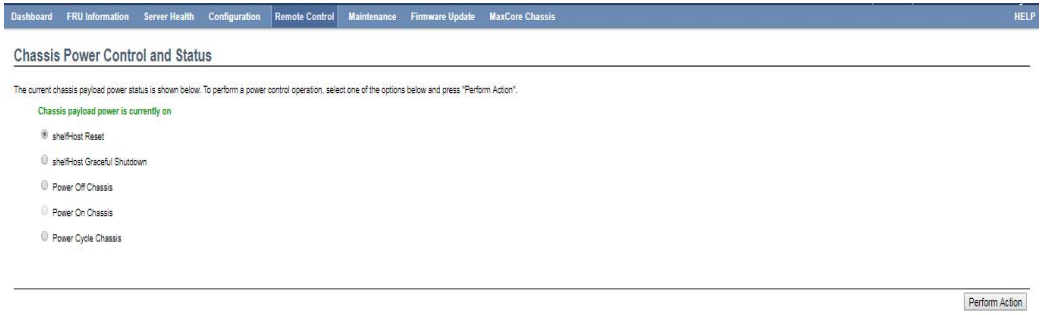
This screen allows you to view and control the power of your server. To open **Chassis Power Control and Status** screen, click **Remote Control** > **Chassis Power & Reset** from the menu bar.

From this screen you can view or perform chassis operations.

Downloaded from Arrow.com.

Figure 7-31 shows the **Chassis Power Control and Status** screen.

Figure 7-32 Chassis Power Control and Status



The following table contains field and button description of **Chassis Power Control and Status** screen.

Table 7-23 Power Control and Status

Field Name	Description
shelfHost Reset	Select this option to reset the MaxCore shelfHost without powering off.
shelfHost Graceful Shutdown	Select this option to attempt to shut down the MaxCore shelfHost gracefully.
Power Off Chassis	Select this option to immediately turn off the MaxCore payload power.
Power On Chassis	Select this option to turn on the MaxCore payload power.
Power Cycle Chassis	Select this option to first turn off, and then turn on the MaxCore payload power.
Perform Action	Performs the action based on the selected option.

Procedure

Select an option from the list and click **Perform Action**.

Downloaded from Arrow.com.

Note: You will be asked to confirm your choice. Upon confirmation, the command will be executed and you will be informed of the status.

7.1.3.7 Maintenance

The **Maintenance** menu contains following items:

- Synchronize Configuration
- Restore Configuration
- System Administrator

7.1.3.7.1 Synchronize Configuration

This feature allows you to synchronize BMC configuration between the current active image and the inactive image by copying the configuration from one image to the other.

Table 7-24 Synchronize Configuration

Field Name	Description
Active-to-Inactive	Copies the current configuration, thxat means the configuration of active image to the inactive image.
Inactive-to-Active	Copies the inactive image's configuration to active image. Reboot is required before it takes effect.

7.1.3.7.2 Restore Configuration

In MegaRAC GUI, this page helps you to restore the configuration of the device.

NOTICE

After entering restore factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

Downloaded from Arrow.com.

Procedure

To restore the firmware configuration with default configuration, click **Restore Configuration** button.

7.1.3.7.3 System Administrator

The **System Administrator** screen enables you to configure the System Administrator settings, such as the root account of the BMC.The default *username* and *password* are *sysadmin*/*superuser* respectively. We strongly recommend you to change the System Administrator password, instead of using default.

NOTICE

Be careful while performing any changes in the system by using root permissions. Any error in these operations may destroy the product consistency and damage the hardware, which would originate support and warranty issues.

Table 7-25 System Administrator

Field Name	Description
Username	Username of System Administrator (it is a read-only field).
User Access	Provides user access for system administrator.
Change Password	Allows you to change the password. **Note**: Password, Confirm Password. ● Password must be at least 8 characters long. ● White space is not allowed. **Note**: This field will not allow more than 64 characters.
Save	Saves the new configuration for system administrator.
Reset	To reset the previously saved values.

Downloaded from Arrow.com.

Procedure

To enable or disable access and change the password for the System Administrator account, perform the following steps:

1. To enable User Access, select the **Enable** option.
2. Select **Change Password** option to change the password. This action enables the password fields.
3. Enter the new password in the **Password** field.
4. Re-enter the password in the **Confirm Password** field.
5. Click **Save** to save the changes or click **Reset** to reset the previously saved values.

7.1.3.8 Firmware Update

You can perform the following tasks under **Firmware Update** menu:

- Firmware Update
- Dual Image Configuration

7.1.3.8.1 Firmware Update

This wizard takes you through the process of firmware upgrade. A reset of the box will automatically follow, if the upgrade is completed or canceled.

NOTICE

After entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If the upgrade process is canceled in the middle of the wizard, the device will be reset.

The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation.

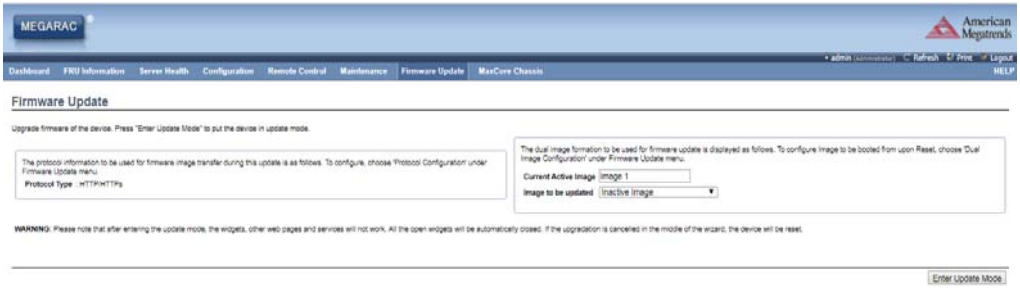
Downloaded from Arrow.com.

Once you enter into Update Mode and choose to cancel the firmware flash operation, the BMC card must be reset. This means that you must close the Internet browser and log back onto the BMC card before you can perform any other types of operations.

Once Firmware upgrade using web is started, the regular IPMI command will not be allowed for safety concern.

To open **Firmware Update** screen, click **Firmware Update** > **Firmware Update** from the menu bar. Figure 7-33 shows the **Firmware Update** screen.

Figure 7-33 Firmware Update



Downloaded from Arrow.com.

The following table describes the field and button description of **Firmware Update** screen.

Table 7-26 Firmware Update

Field Name	Description
Current Active Image	Displays the name of current active Image.
Image to be uploaded	List of images to be uploaded. If required, you can choose both the images.
Enter Update Mode	Allows you to update the firmware of the current device.

NOTICE

After entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If the upgrade process is canceled in the middle of the wizard, the device will be reset.

Procedure

To upgrade the firmware of the current device, perform the following steps:



You need dual image information for firmware updates. So, to configure image to reboot from upon Reset, refer to the section *Dual Image Configuration* on page 193.

1. Do not modify the image selected to be updated from **Image to be updated** drop-down list. Never overwrite the image the BMC has booted from.
2. Select **Reboot the device after update** check box.

Downloaded from Arrow.com.

3. On the **Firmware Update** page, click **Enter Update Mode** to upgrade the current device firmware. The Firmware update process closes all active client requests, prepares device for firmware upgrade and then allows to upload Firmware image by displaying the **Upload Firmware** screen.

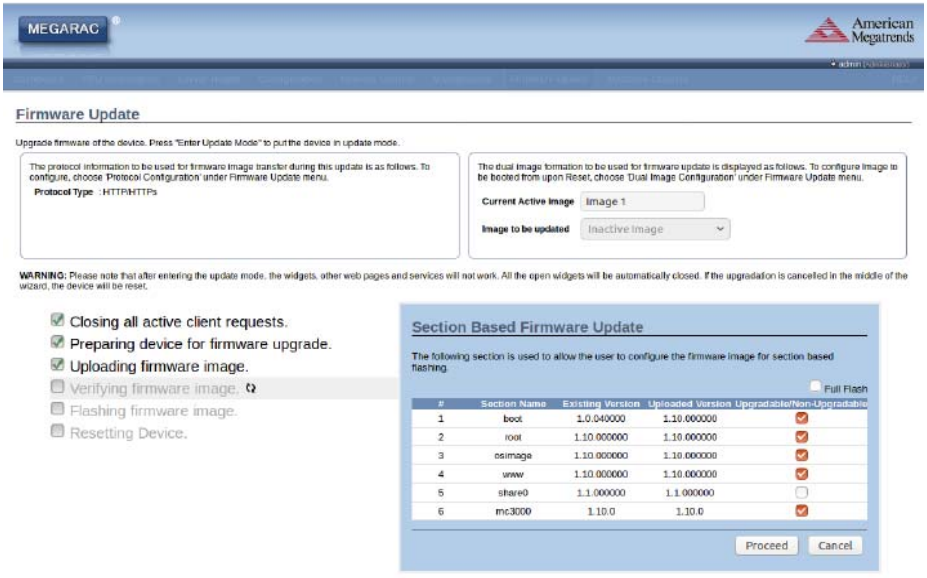
Figure 7-34 Upload Firmware



Downloaded from Arrow.com.

4. Click **Browse** to select the Firmware image to flash and then click **Upload**. The **Section Based Firmware Update** screen is displayed. You can configure the firmware image for section based flashing here.

Figure 7-35 Section Based Firmware Update



Element Name	Description
Full Flash	Select this option, if flashing is required for all images. **Note**: ARTESYN recommends performing a Full Flash Update always.
Section Name	Name of the section
Existing Version	Existing firmware version number.
Uploaded Version	Uploaded firmware version number.
Upgradeable/Non-Upgradeable	Allows to set whether the firmware version can be upgradeable or not.

Downloaded from Arrow.com.

Only selected sections of the firmware will be updated. Other sections are skipped. Before starting flash operation, verify the compatibility between image sections.

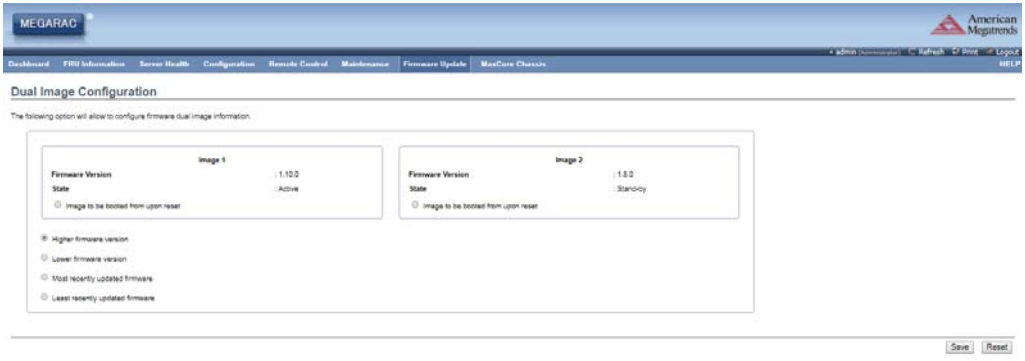
5. Select the required options and click **Proceed** to update the firmware.

7.1.3.8.2 Dual Image Configuration

You can configure the dual image information here. Dual Image support feature allows you to store two firmware images on two 64MB SPIs and boot any of the image according to user's request. The running firmware is responsible for setting the Boot Selector and Firmware Upload Selector options.

To open **Dual Image Configuration** screen, click **Firmware Update** > **Dual Image Configuration** from the menu bar.

Figure 7-36 Dual Image Configuration



The following table contains field and button description of **Dual Image Configuration** screen.

Table 7-27 Dual Image Configuration

Field Name	Description
Firmware Version	Displays the firmware version of both images.

Downloaded from Arrow.com.

Table 7-27 Dual Image Configuration

Field Name	Description
State	Displays the current state of both images. One would be in Active and would be in Stand-by mode.
Image to be booted from upon reset	Boots the selected image (either 1 or 2) in the next boot up process.
Higher firmware version	Boots higher firmware version image among the dual images in the next boot up process.
Lower firmware version	Boots lower firmware version image among the dual images in the next boot up process.
Most recently updated firmware	Boots most recently updated firmware image among the dual images in the next boot up process.
Least recently updated firmware	Boots least recently updated firmware image among the dual images in the next boot up process.
Save	Saves the configured settings.
Reset	Clears the previously saved values.

Procedure

1. Select the required image to be configured or the required option for Image setting.
2. Click **Save** to save the changes.

7.1.3.9 MaxCore Chassis

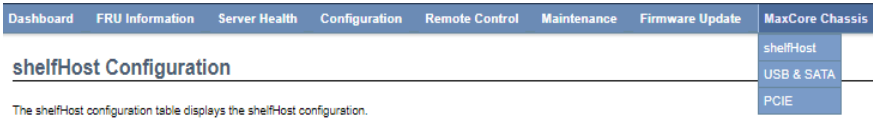
From the **MaxCore Chassis** menu, you can perform the following tasks:

- shelfHost Configuration
- USB & SATA Configuration
- PCIe Configuration

Downloaded from Arrow.com.

Figure 7-37 shows the **MaxCore Chassis** menu options.

Figure 7-37 MaxCore Chassis Menu



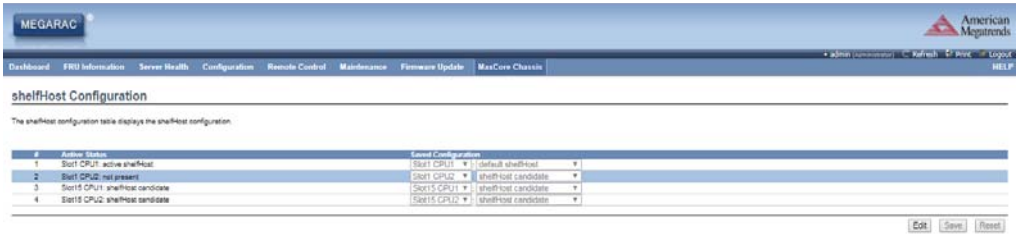
7.1.3.9.1 shelfHost

The shelfHost CPU is the first to be booted in the chassis.

To open **shelfHost** page, click **MaxCore Chassis** > **shelfHost** from the menu bar. On the **shelfHost Conifguration** screen, you can view current shelfHost election status and shelfHost configuration file settings.

Figure 7-33 shows **shelfHost Configuration** screen.

Figure 7-38 shelfHost Configuration



The following table describes field and button description of **shelfHost Configuration** screen.

Table 7-28 shelfHost Configuration

Field Name	Description
Active Status	Displays status of CPUs in Slot 1 and Slot 15.
Saved Configuration	Displays the saved configuration information.
Edit	Allows you to modify the configuration.

Downloaded from Arrow.com.

Table 7-28 shelfHost Configuration

Field Name	Description
Save	Saves the changes.
Reset	Resets the modified configuration changes to default configuration.

Procedure

To modify the shelfHost Configuration, perform the following steps:

1. Click **Edit** button to enable options under **Saved Configuration**.
2. Perform the required changes and click **Save** to save the changes. A message box pops-up on the screen.
3. Click **OK** to continue.

7.1.3.9.2 USB & SATA

To open **USB & SATA** page, click **MaxCore Chassis** > **USB & SATA** from the menu bar. On the **USB & SATA Conifguration** screen, you can view current SATA Ports assignment to the manageable CPUs in Slot1 and Slot15.

Figure 7-33 shows **USB & SATA Configuration** screen.

Figure 7-39 USB & SATA Configuration



Downloaded from Arrow.com.

The following table describes field and button description of **USB & SATA Configuration** screen.

Table 7-29 USB & SATA Configuration

Field Name	Description
Port	Displays the list of ports.
Active Status	Displays the status of each port.
Saved Configuration	Displays current port configuration.
Edit	Allows you to modify the configuration
Save	Saves the changes.
Reset	Resets the modified configuration changes to default configuration.

Procedure

To modify the USB & SATA Configuration, perform the following steps:

1. Click **Edit** button to enable options under **Saved Configuration**.
2. Perform the required changes and click **Save** to save the changes. A message box proceed pops-up on the screen.
3. Click **OK** to continue.

7.1.3.9.3 PCIe Configruation

From the **PCIe Configuration** screen, you can reset the PCIe configuration.

To open **PCIe Configuration** page, click **MaxCore Chassis** > **PCIE** from the menu bar.

Downloaded from Arrow.com.

The following table describes field and button description of **PCIe Configuration** screen.

Table 7-30 PCIe Configuration

Field Name	Description
Reset PCIe Configuration to Default	Allows you to reset the PCIe configuration to the default. The default configuration sets the PCIe to Fabric mode with CPU1 in Slot1 as the shelfHost **Note**: This options is only for emergency purpose. It is suggested to use the System Services Framework (SSF) or the `mccs_tool.py` option.

7.1.3.10 Log Out

To log out of the MegaRAC GUI, click **Logout** button on the top right corner of the screen.

7.2 Serial Over LAN

MaxCore provides network access to the serial interface for a selected CPU within MaxCore. That CPU can be any CPU on a PCIE-7410 or PCIE-9205 card. This feature is called Serial Over LAN (SOL).

There are two methods to open a console window on a remote PC.

- Executing *ipmitool* utility. This works for Linux PCs, but it is not available for Windows PCs.
- Executing any type of ssh capable terminal emulator.
  You can find a better terminal emulator from putty.org. These terminal emulators are basically available for all types of OSes on both PCs and mobile devices.

MaxCore supports one SOL session at a time. The following sections describe how to setup a serial console session to your selected CPU.

Before doing that it is important to understand that each CPU on a PCIE-7410 or PCIE-9205 has two serial ports. The **ttyS0**/**COM1** is connected to the microUSB connector at the card bracket. The **ttyS1**/**COM2** is used for SOL. The BIOS of these CPUs will always show up at both ports. A Linux OS must be configured to use either the one or the other. The OS installation procedures in this manual describe this selection process.

Downloaded from Arrow.com.

7.2.1 SOL via IPMI

Serial Over LAN (SOL) is implemented in the BMC with LAN channel #1 and LAN channel #3.

LAN channel #1, by default, provides serial access to the system host via BMC ETH RJ45. This can be through the serial console of the system host CPU residing either at slot #1 or at slot #15. The serial console selection depends on the system host election process, for more information see *Set shelfHost Configuration Table* on page 217.

Instead of using LAN channel #1, LAN channel #3 can be used alternatively. For more details, see *Establishing SOL to any System Host Micro Server Card* on page 200.

The BMC provides two LAN channels:

- LAN channel #1: Accessed via BMC ETH RJ45, powered with management power.
  Default IP: *192.168.201.9*
- LAN channel #3: Accessed via ETH4 RJ45, powered with payload power.
  Default IP: 172.26.1.1

SOL can be activated at any of the LAN channels using the following command. The *ipmitool* can be downloaded from https://sourceforge.net.

```
# ipmitool -I lanplus -H 192.168.201.9 -U admin -P admin sol
activate
```

NOTICE

The BMC Ethernet interface BMC ETH RJ45 is an internal network interface, which is meant for internal management purpose. It shall not be routed to the public network for security purpose.

The default baud rate of the SOL channel is 38400.

7.2.1.1 Configuring BIOS

The BIOS need to be configured such that the second serial console COMB is enabled, otherwise no serial output can be displayed by the BMC.

Downloaded from Arrow.com.

To configure BIOS to redirect serial output to the BMC, perform the following steps:

1. Enter **BIOS setup**.
2. Go to **Advanced** menu, and click **Serial Redirection** tab.
3. Enable COMB interface.

7.2.1.2 Configuring OS

By default, the OS does not redirect its second serial interface to the BMC. So, there is no serial output seen at the BMC. To enable serial redirection, you need to set the second serial interface in the GRUB file, explained in the following procedure:

1. Open the *grub.cfg* file.
2. Check for the kernel line, which corresponds to your currently running kernel.
3. Add or modify the *console* parameter as shown below.

```
console=ttyS0,38400  -     Standard console output
console=ttyS1,38400  -     Console output via SOL
```

4. Save the changes.

7.2.1.3 Establishing SOL to any System Host Micro Server Card

The SOL channel is not connected to a particular serial interface. The serial interface redirected to the BMC can be changed during an active SOL session. By default, the serial interface of the system host is redirected to the BMC. This can be changed with the IPMI OEM command Set FRU Instance Serial Route. For more information, refer to the section *Set FRU Instance Serial Route* on page 224.

The following is an example to select CPU 2 at slot 1. Select UART #1 for the first SOL session and UART #2 for the second SOL session.

```
# ipmitool -I lanplus -H 192.168.201.9 -U admin -P admin raw 0x2e
0x38 0xae 0x00 0x01 0x03 0x61 0x01
```

7.2.2 SOL via SSH

This option enables direct SOL over ssh without the need for IPMI.

```
# ssh admin@192.168.201.9
```


Downloaded from Arrow.com.

```
# /opt/fru/bin/sol <slot ID> <CPU ID>
```

The following is an example to select CPU 2 at slot 5.

```
# /opt/fru/bin/sol 5 2
```

Alternatively, SOL sessions can be established to each CPU in the MaxCore system. The valid values for Slot ID are 1-15 and for CPU ID are 1-2.

7.3 Remote KVM and Media

KVM means Keyboard, Video, and Mouse. The MegaRAC Remote Console application allows you to control the operating system of the MaxCore management CPU remotely using the screen, mouse, and keyboard, and to redirect local CD/DVD, floppy diskette, and hard disk/USB thumb drives as if they were connected directly to the server. This specific feature is not supported for any other CPU in MaxCore. The SOL feature provides console access for such CPUs.



To launch KVM, disable the pop-up blocker of your web browser. In the Internet Explorer, enable the download file options from the settings.

The Remote Console is an OS independent Java plug-in that can be used in Windows as well as Linux with the help of the Java Runtime Environment (JRE). JRE must be installed in the client's system. You can install JRE from http://www.java.com.

7.3.1 Invocation Procedure

In MegaRAC GUI, you can launch Remote Console in two ways:

- In the **Dashboard** page and click **Launch** button inline with **Remote Control**.
- Go to **Remote Control** > **Console Redirection** and then click **Java Console**.

Downloaded from Arrow.com.

This will load a Java application from the BMC and will also launch the JRE to run this application.The JRE will not run an application from an unknown source. In such case, use the **Java Control Panel** to change the security settings add the BMC's IP address to the **Java Site List**.

A new **JViewer** window pops up with a set of pull-down menus and the remote console. Select the **JViewer** window and press <Enter> to see the text or graphical message of your OS.

Procedure

To connect a remote media for the next boot, perform the following steps:

1. In the **JViewer** window, go to **Media** > **Virtual Media Wizard** to display **Virtual Media window.**
2. Select your possible virtual media. For example, Floppy key, CD/DCVD, HDD or USB.
3. Click **Browse** inline with the selected virtual media (for example, *.iso* for CD and *.img* for HDD) and click the **Connect <Virtual Media>** button.
4. Reboot the CPU (In the **MegaRAC** application, go to **Remote Control** > **Server Power Control**, select **Reset Server** option and click **Perform Action** button).
5. Enter the BIOS boot console by pressing <F4> (remote console in JViewer).

7.3.2 Reference Guide

The **JViewer** menu bar consists of the following menu items:

- Video
- Keyboard
- Mouse
- Options
- Media
- Keyboard Layout
- Video Record

Downloaded from Arrow.com.

- Power
- Active Users
- Help

A detailed explanation of these menu items is given below.

7.3.2.1 Video

This menu contains the following sub menu items.

Table 7-31 Video menu

Field name	Description
Pause redirection	Pauses the Console Redirection.
Resume Redirection	Resumes the Console Redirection when the session is paused.
Refresh Video	Updates the display shown in the Console Redirection window.
Turn OFF Host Display/ *Host Video Output	If you enable this option, the server display will be blank, but you can view the screen in Console Redirection. If you disable this option, the display will be back in the server screen.
Capture Screen	Helps to capture the screenshot of the host screen and save it in the client's system.
Full Screen	Allows you to view the Console Redirection in full screen mode (Maximize). This menu is enabled only when both the client and host resolution are same.
Exit	Exits the console redirection screen.

Downloaded from Arrow.com.

7.3.2.2 Keyboard

This menu contains the following sub menu items.

Table 7-32 Keyboard menu

Field name	Description
Hold Right Ctrl Key	Acts as the right-side <CTRL> key when in Console Redirection.
Hold Right Alt Key	Acts as the right-side <ALT> key when in Console Redirection.
Hold Left Ctrl Key	Acts as the left-side <CTRL> key when in Console Redirection.
Hold Left Alt Key	Helps to take the screenshot of the host screen and save it in the client's system.
Left Windows Key	Acts as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: **Hold Down** or **Press and Release**.
Right Windows Key	Acts as the right-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: **Hold Down** or **Press** and **Release**.
Ctrl+Alt+Del	Acts as if you depressed the <CTRL>, <ALT>, and <DEL> keys down simultaneously on the server that you are redirecting.
Context menu	Acts as the context menu key, when in Console Redirection.
Hot Keys	Adds the user configurable shortcut keys to invoke in the host machine. The configured key events are saved in the BMC.
Full Keyboard Support	Enable this option to provide full keyboard support. Used to trigger the <Ctrl> and <Alt> key directly to host from the physical keyboard.

7.3.2.3 Mouse

Mouse menu contains the following sub menu items.

Table 7-33 Mouse menu

Field name	Description
Show Cursor	Shows or hides the local mouse cursor on the remote client system.

Downloaded from Arrow.com.

Table 7-33 Mouse menu (continued)

Field name	Description
Mouse Calibration	Used only if the mouse mode is relative. In this step, the mouse threshold settings on the remote server will be discovered. The local mouse cursor is displayed in RED color and the remote cursor is part of the remote video screen. Both the cursors will be synchronized in the beginning. Use '+' or '-' keys to change the threshold settings until both the cursors go out of synch. Detect the first reading on which cursors go out of synch. Once this is detected, use <ALT + T> to save the threshold value.
Mouse Mode	Handles mouse emulation from local window to remote screen using either of the two methods. Only *Administrator* has the right to configure this option. ● **Absolute mouse mode**: The absolute position of the local mouse is sent to the server, if this option is selected. ● **Relative mouse mode**: The relative mode sends the calculated relative mouse position displacement to the server, if this option is selected. ● **Other mouse mode**: This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation. **Note**: Client cursor will be hidden always. If you want to enable, use <Alt + C> to access the menu.

Downloaded from Arrow.com.

7.3.2.4 Options

This menu contains the following sub menu items.

Table 7-34 Options menu

Field name	Description
Band width	**Auto Detect**: Detects the network bandwidth usage of the BMC automatically. The Bandwidth Usage option allows you to adjust the bandwidth. You can select one of the following: ● 256Kbps ● 512Kbps ● 1Mbps ● 10Mbps
Keyboard/Mouse Encryption	Allows you to encrypt keyboard inputs and mouse movements sent between the connections.
Zoom	**Note**: This option is available only when you launch the Java Console. ● **Zoom In** – For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%. ● **Zoom Out** – For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%. ● **Actual Size** – By default, this option is selected. **Fit to Client Resolution**: If the host screen resolution is greater than the client screen resolution, choose this option to fit the host screen to client screen. **Fit to Host Resolution**: If the host screen resolution is lesser than the client screen resolution, choose this option to resize the JViewer frame to the host resolution.
Send IPMI Command	Allows to display the **IPMI Command** dialog. Enter the raw IPMI command in **Hexadecimal** field as Hexadecimal value and click **Send**.
GUI Languages	You can choose the desired GUI language.

Downloaded from Arrow.com.

Table 7-34 Options menu (continued)

Field name	Description
Request Full Permission	Partially Permitted sessions can use this option to request the full permission from the existing full permitted session. **Note**: This menu option is available only for partially privileged session and Full permission sessions will not have this option in the menu.

Downloaded from Arrow.com.

7.3.2.5 Media

This menu contains the following sub menu items.

Table 7-35 Media menu

Field name	**Description**
Floppy Key Media	Starts or stops the redirection of a physical floppy drive and floppy image types such as *img*. **Note**: Floppy Redirection is not an available feature on all versions of the MegaRAC® SPXs.
CD/DVD Media	Starts or stops the redirection of a physical DVD/ CD-ROM drive and CD image types such as ISO.
Hard disk/USB Key Media	Starts or stops the redirection of a Hard Disk/USB key image and USB key image such as *img*. **Note**: For redirecting Floppy and Hard disk drives, the user should have administrator privilege (root user in the case of Linux clients).



- **For Windows 7 or later, the web browser from which the KVM redirection will be initiated, should be launched using *Run as Administrator* option. If there are multiple instances of the web browser open simultaneously, ensure that all the instances are launched using the *Run as Administrator* option.**
- **For Windows client, if the logical drive of the physical drive is dismounted then the logical device is redirected with Read/Write Permission, else it is redirected with Read permission only.**
- **For MAC client, only External USB Hard disk redirection is supported.**
- **For Linux client, fixed hard drive is redirected only as Read Mode. It is not Write mode supported.**
- **For USB key image redirection, support FAT 16, FAT 32, and NTFS.**
- **SPX Stack Media redirection supports only Basic Hard disk Redirection.**

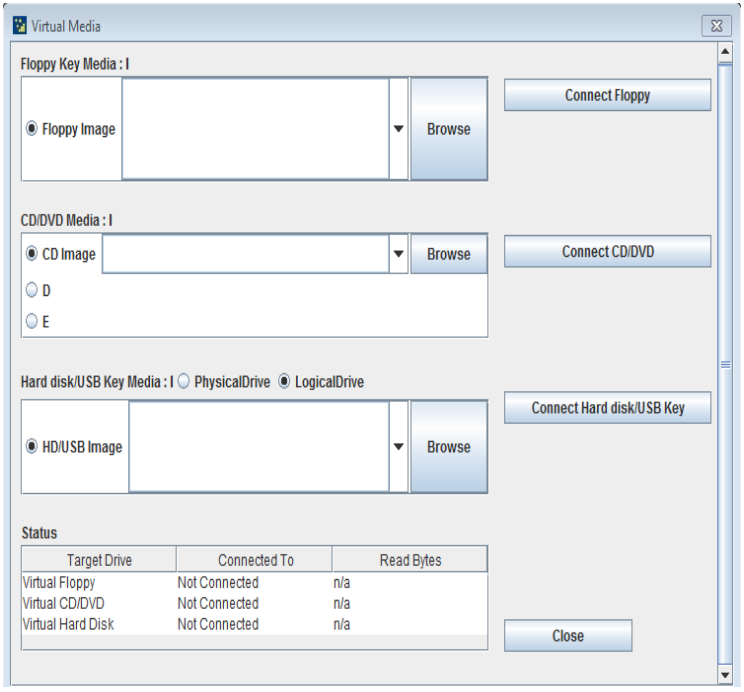
Downloaded from Arrow.com.

Procedure

To connect to the remote media:

1. Go to **Media** > **Virtual Media Wizard** to display **Virtual Media window**.You can select the required virtual media options here.

Figure 7-40 Virtual Media



2. Click **Browse** button inline with the list of media options to set the location of the respective media image.

3. Click **Connect <Virtual Media Type>** button inline with selected Virtual media image.
   After connecting to the required virtual media device with image, close the window. The **Connect <Virtual Media Type>** is a toggle button.

Downloaded from Arrow.com.

4. Reboot the CPU (In the **MegaRAC** application, go to **Remote Control** > **Server Power Control**, select **Reset Server** option and click **Perform Action** button).
5. Enter the BIOS boot console by pressing <F4> to select the just connected device for the next boot.

7.3.2.6 Keyboard Layout

This menu contains the following sub menu items.

Table 7-36 Keyboard menu

Field name	Description
Auto Detect	This option is used to detect keyboard layout automatically. The languages supported automatically are English – US, French – France, Spanish – Spain, German- Germany. If the client and host languages are same, then for all the languages other than English mentioned above, you must select this option to avoid typo errors. If the host and client languages differ, you can choose the host language layout in the menu and thereby can directly use the physical keyboard.
Host Physical Keyboard	This option allows you to select the keyboard layout. You must select the appropriate language in the list shown in JViewer. We have list of the language supported: 1. English –US 2. English – UK 3. Spanish 4. German 5. Italian 6. Danish 7. Finnish 8. French 9. Dutch 10. Russian 11. Japanese 12. Turkish

Downloaded from Arrow.com.

Table 7-36 Keyboard menu (continued)

Field name	Description
Soft Keyboard	This option allows you to select the keyboard layout. It will show the dialog as similar to onscreen keyboard. If the client and host languages are different, then for all the languages other than English mentioned above, you must select the appropriate language in the list shown in JViewer and use the soft keyboard to avoid typo errors. We have list of the language support in JViewer. 1. English –US 2. English – UK 3. Spanish 4. German 5. Italian 6. Danish 7. Finnish 8. French 9. Dutch 10. Russian 11. Japanese 12. Turkish **Note**: Soft keyboard is applicable only for JViewer Application not for other application in the client system.

7.3.2.7 Video Record

This menu contains the following sub menu items.

Table 7-37 Video Record menu

Field name	Description
Start Record	To start recording the screen.
Stop Record	To stop the recording.
Settings	To set the settings for video recording.

Downloaded from Arrow.com.

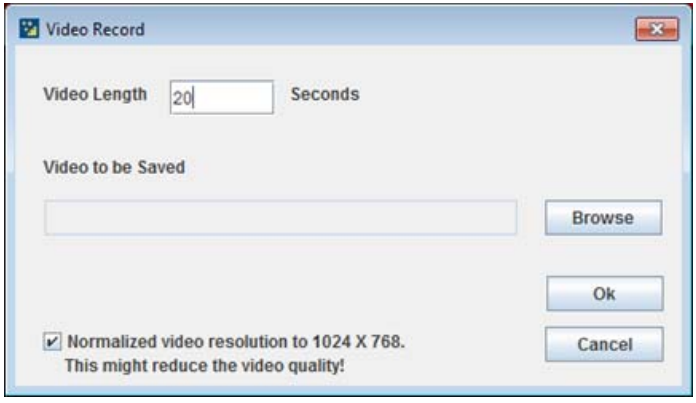
Procedure

To record a video, perform the following steps:

Note: Before you start recording, you have to enter the settings.

1. Click **Video Record** > **Settings** to open the settings page as shown in the screenshot below.

Figure 7-41 Video Record Settings Page



2. Enter the length of the video in seconds.
3. Click **Browse** and the enter the location where you want the video to be saved.
4. Enable the **Normalized video resolution to 1024X768** option by clicking the checkbox.
5. Click **OK** to save the entries and return to the **Console Redirection** screen or click **Cancel** to discard the changes.
6. In the **Console Redirection** window, click **Video Record** > **Start Record** to start the video recording.
7. To stop the recording, click **Video Record** > **Stop Record**.

Downloaded from Arrow.com.

7.3.2.8 Power

The power option is to perform any power cycle operation. Click the required option to perform the following operation.

Table 7-38 Power menu

Field name	Description
Reset Server	To reboot the system without powering off (warm boot).
Immediate Shutdown	To immediately power off the server.
Orderly Shutdown	To initiate operating system shutdown prior to the shutdown.
Power On Server	To power on the server.
Power Cycle Server	To first power off, and then reboot the system (cold boot).

7.3.2.9 Active Users

This menu displays the active users and their system IP address.

7.3.2.10 Help

This menu displays the copyright and version information.

7.3.2.11 Quick Buttons

The lower right of **Console Redirection** window displays all the quick buttons. These quick buttons helps you to perform these functions by just clicking them.

Note: This option is available only when you launch the Java Console.

Table 7-39 Quick buttons

Quick Buttons	Explanation
	Play the Console redirection after being paused.

Downloaded from Arrow.com.

Table 7-39 Quick buttons

Quick Buttons	Explanation
	Used for pausing Console Redirection.
	To view the Console Redirection in full screen mode. **Note**: Set your client system resolution same to host system resolution so that you can view the server in full screen.
	To show or hide the soft keyboard.
	Drag this to zoom in or out.
	To record the video.
	These three quick buttons will pop up a virtual media where you can configure the media.
	To show or hide the mouse cursor on the remote client system.
	Displays the details of Active Users.
	This button will work like toggle button. If the icon is in Green color server status is power on. By clicking the button immediate shutdown action will be triggered in host. If the icon is in Red color, server status is power off. Click the button to power on the host.
	Displays the available hotkeys.

Downloaded from Arrow.com.

7.4 OEM Commands

All Artesyn-specific OEM commands have the network function code **0x2e**/**0x2f**. The group extension code is **0xae**.

The first data byte position in requests and responses (after the completion code) under this network function identify Artesyn as defining body. The data byte is the group extension code.

The following table provides the general OEM structure information.

Table 7-40 General OEM Command Structure

	Byte	Data
Request Data	1	0xae
	2	Version of command/message
	n	Request payload data, *n* bytes
Response Data	1	Completion Code
	2	0xae
	m	Response payload data, *m* bytes

7.4.1 OEM Command Summary

The following table provides OEM commands information.

Table 7-41 OEM Command Summary

Command	NetFn	Command Code	Description
Set shelfHost Configuration Table	OEM/Group	0x30	*Set shelfHost Configuration* on page 217
Get shelfHost Configuration Table	OEM/Group	0x31	*Get shelfHost Configuration* on page 218
Set FRU Instance Power State	OEM/Group	0x34	*Set FRU Instance Power State* on page 220
Get FRU Instance Power State	OEM/Group	0x35	*Get FRU Instance Power State* on page 221

Downloaded from Arrow.com.

Table 7-41 OEM Command Summary (continued)

Command	NetFn	Command Code	Description
Set Chassis Power Policy	OEM/Group	0x36	*Set Chassis Power Policy* on page 222
Get Chassis Power Policy	OEM/Group	0x37	*Get Chassis Power Policy* on page 222
Set FRU Instance Serial Route	OEM/Group	0x38	*Set FRU Instance Serial Route* on page 224
Get FRU Instance Serial Route	OEM/Group	0x39	*Get FRU Instance Serial Route* on page 225
Set BMC Feature Configuration	OEM/Group	0x4C	*Set BMC Feature Configuration* on page 226
Get BMC Feature Configuration	OEM/Group	0x4D	*Get BMC Feature Configuration* on page 227

7.4.2 shelfHost Configuration

The shelfHost configuration table defines the set of cards and CPUs that are marked as *Available* for shelfHost election. The BMC will try to bring up the card/CPU which is listed at the first position of the table. If that card/CPU is not available then the BMC continues with the next entry. Therefore, the order in the table defines the priority of which CPU is elected first and so on. If there are no more entries left in the table then the BMC aborts the power-up and initialization sequence and generates an event in the SEL. A default system host configuration table is provided below, which applies if there is no user-defined table found or defined.

shelfHost election happens whenever the shelf payload power is switched ON.The shelfHost failure policy defines what happens when the shelfHost fails. The default policy is to switch off shelf payload.

Downloaded from Arrow.com.

7.4.2.1 Default shelfHost Configuration

The following table provides the default shelfHost configuration information.

Table 7-42 Default shelfHost Configuration

FRU	CPU Instance	State
FRU/Slot 1	1	Active
FRU/Slot 1	2	CPU2 should not be not a candidate by default.
FRU/Slot 15	1	Available
FRU/Slot 15	2	CPU2 should not be not a candidate by default.

7.4.2.2 Set shelfHost Configuration

The following table provides the set shelfHost configuration information.

Table 7-43 Set shelfHost Configuration Table

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification.
	3	Number of entries n 4 for this specification.

Downloaded from Arrow.com.

Table 7-43 Set shelfHost Configuration Table (continued)

	Byte	Data
Entry x with x from 0..(n-1), only if n > 0	3+4*x	FRU/slot ID of card
	3+4*x+1	Entity ID code on card. For processors this should be 0x03.
	3+4*x+2	Entity instance number on card. The first processor has the instance number 0x60.
	3+4*x+3	[7:5] Reserved [4:0] State code: 0: CPU not available 1: CPU available 4: CPU is system host Other values are reserved.
Response Data	1	Completion Code
	2	0xae

7.4.2.3 Get shelfHost Configuration

The following table provides the get shelfHost configuration information.

Table 7-44 Get shelfHost Configuration

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification
	(3) Optional	Parameter set to return: 0: actual configuration table 1: stored configuration table
Response Data	1	Completion Code
	2	0xae

Downloaded from Arrow.com.

Table 7-44 Get shelfHost Configuration (continued)

	Byte	Data
	3	Number of entries n 4 for this specification
Entry x with x from 0..(n-1), only if n > 0	4+4*x	FRU/slot ID of card
	4+4*x+1	Entity ID code on card. For processors this should be 0x03.
	4+4*x+2	Entity instance number on card. The first processor has the instance number 0x60.
	4+4*x+3	[7:5] Reserved [4:0] State code: 0: CPU not available 1: CPU available 2: CPU marked as failed 3: CPU not present 4: CPU currently serving as system host

The third parameter of the Request Data is optional, if it is omitted, the actual configuration table will be returned.

7.4.3 Power Management

As far as an FRU provides power management, it can be determined with a set of commands explained in the following sections.

Downloaded from Arrow.com.

7.4.3.1 Set FRU Instance Power State

The following table provides set FRU instance power state information.

Table 7-45 Set FRU Instance Power State

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification
	3	FRU/slot ID of card 1-15: card in a PCIe-slot
	4	Entity ID code on card or slot. 0x03: Entity processor 0x90: Entity PCIe slot
	5	Entity instance number on FRU. For entity 0x03 processor: 0x60+x: CPU x on the card (FRU1-15). x starts from 0. For entity 0x90 PCIe-slot: 0x60: entire slot
	6	[7:5] reserved [4:0] Power State: 0: power down 1: power up 2: reset Other values are reserved. For processor entities a reset of the CPU is performed. For a PCIe slot entity a reset performs a #PERST of the slot.
Response Data	1	Completion Code
	2	0xae

Downloaded from Arrow.com.

7.4.3.2 Get FRU Instance Power State

The following table provides get FRU instance power state information.

Table 7-46 Get FRU Instance Power State

	Byte	Data
Request Data	1	0xae
	2	version 0 for this specification
	3	FRU Device ID. 1 – 15: the PCIe card in the corresponding slot.
	4	Entity ID code on card or slot 0x03: Entity processor 0x90: Entity PCIe slot
	5	Entity instance number on card. For Entity 0x03 processor: 0x60+x: CPU x on the card (FRU1-15). x starts from 0. For Entity 0x90 PCIe slot: 0x60: entire slot
Response Data	1	Completion Code
	2	0xae
	3	[7:5] reserved [4:0] Power State: 0: power down 1: power up 2: reset 3: not present For processor entities, a reset of the CPU is performed. For a PCI slot entity, a reset performs the #PERST of the slot.

Downloaded from Arrow.com.

7.4.3.3 Set Chassis Power Policy

The chassis power policy specifies how the system is powered when it comes up. The following table provides set chassis power policy information.

Table 7-47 Set Chassis Power Policy

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification
	3	Power policy: [0]: payload power (1=Enabled) [1]: power loss (1=Payload power cannot be enabled, if power loss has happened before. Subsequent power on will power the BMC only. This setting is persistent until this command is executed again).
Response Data	1	Completion Code
	2	0xae

7.4.3.4 Get Chassis Power Policy

The following table provides get chassis power policy information.

Table 7-48 Get Chassis Power Policy

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification

Downloaded from Arrow.com.

Table 7-48 Get Chassis Power Policy

	Byte	Data
Response Data	1	Completion Code
	2	0xae
	3	Power policy: [0]: payload power (1=Enabled) [1]: power loss (1=Payload power cannot be enabled, if power loss has happened before. Subsequent power-on will power the BMC only. This setting is persistent until this command is executed again).

7.4.4 FRU UART Management

MaxCore provides a serial redirection method for Artesyn PCIe cards, residing at any slot, to provide Serial Over Lan (SOL). The following commands are used to select a dedicated serial interface instance to be routed to the BMC.

Currently, SOL connections can be established only via UART #1. Additional UARTs can be routed to the BMC, but currently they are not supported.

Downloaded from Arrow.com.

7.4.4.1 Set FRU Instance Serial Route

The following table provides set FRU instance serial route information.

Table 7-49 Set FRU Instance Serial Route

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification
	3	FRU Device ID 1 – 15: the PCIe card in the corresponding slot. Other values are reserved.
	4	Entity ID code on card For processors this should be 0x03.
	5	Entity instance number on card 0x60+x: CPU x on the card (FRU1-15). x starts from 0. The first processor has the instance number 0x60.
	6	[7:5] reserved [3:0] UART: 0: disabled 1: BMC UART1 for Serial-over-LAN Other values are reserved.
Response Data	1	Completion Code
	2	0xae

Downloaded from Arrow.com.

7.4.4.2 Get FRU Instance Serial Route

The following table provides get FRU instance serial route information.

Table 7-50 Get FRU Instance Serial Route

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification
	3	FRU/slot ID of card
	4	Entity ID code on card For processors this should be 0x03.
	5	Entity instance number on card
Response Data	1	Completion Code
	2	0xae
	3	[7:4] reserved [3:0] UART: 0: disabled 1: BMC UART1 for Serial-over-LAN Other values are reserved.

7.4.5 Configuring BMC Features

This features is used to configure BMC specific features. The first feature implemented with BMC firmware v1.6.8 is called Failover Cluster.

Failover Cluster is a set of two system management CPUs, one defined as active and the other as standby, used to failover MaxCore system management from active system management CPU to the standby system management CPU when booting the active system management CPU fails.

Downloaded from Arrow.com.

Failover Cluster requires Boot Supervision to be enabled. To enable Boot Supervision, the following BMC watchdog configuration mentioned in Table 7-51 on page 226 must be set in the **BIOS setup menu > Advanced > H20 IPMI Configuration > BMC Configuration** screen.

Table 7-51 BMC watchdog configuration

Parameter	Setting
Watchdog Timer Support	Enabled
Watchdog Timer Timeout	8
Watchdog Timer Action	Hard Reset

Failover Cluster furthermore requires that the host configuration table is set in such a way that one CPU is set to active role and the other one to be used with failover cluster is set to standby role. For more details, see Table 7-43 on page 217 in section *shelfHost Configuration* on page 216.

7.4.5.1 Set BMC Feature Configuration

The following table illustrates the command parameter required for Set BMC Feature Configuration.

Table 7-52 Set BMC Feature Configuration

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification
	3	Feature Configuration: [0]: Failover Cluster (1=Enabled) [1:7]: Reserved
Response Data	1	Completion Code
	2	0xae

Downloaded from Arrow.com.

7.4.5.2 Get BMC Feature Configuration

The following table illustrates the command parameter required for Get BMC Feature Configuration.

Table 7-53 Get BMC Feature Configuration

	Byte	Data
Request Data	1	0xae
	2	Version 0 for this specification
Response Data	1	Completion Code
	2	0xae
	3	Feature Configuration: [0]: Failover (1=Enabled) [1..7]: Reserved

7.5 MaxCore Firmware Upgrade

There are several firmware elements in a MaxCore system that may need upgrades throughout the product's life cycle. Some firmware elements are part of the system itself and some reside on PCIe cards. This section provides information on how to upgrade the firmware elements that are part of the system only. The following is the list of firmware elements that come under this group:

- BMC firmware
- Glue CPLD logic
- Companion CPLD logic
- IO-Module CPLD logic

Downloaded from Arrow.com.

This section is not intended to describe the firmware upgrades for elements on Artesyn PCIe cards. You can ignore this section, if you are using Artesyn's SSF to upgrade Firmware components. SSF is the preferred method to upgrade the MaxCore firmware. For more information on software update, refer to *SSF on MaxCore MC3000 Platform GUI Help*.



All the examples provided in the following sections are by assuming default BMC's IP address as *192.168.201.9*. If the address is modified (for example, via the WEB interface) replace the default with the modified address accordingly in the examples.

7.5.1 Obtaining Revisions of Firmware Components

The firmware upgrade of a firmware component is necessary only if firmware components are not found to be up-to-date.

NOTICE

if any of the upgrades is due, it is strongly recommended to upgrade all the firmware elements to their respective versions listed in the latest *SSF for MaxCore MC3000 Release Notes*.
Performing only selective firmware upgrades is not recommended, because this may lead to incompatibilities between the BMC firmware version and CPLD logic elements.

You can manage the system firmware elements as HPM.1 components. You can determine the revision of the HPM.1 firmware components using the tool called *ipmitool*. You can download it from http://ipmitool.sourceforge.net.



There are different versions of *ipmitool* available, each using different command sets to the BMC. MaxCore has been tested with *ipmitool* version v.1.8.14 and it is strongly recommended to use this version of *ipmitool* in order to avoid errors when communicating with the BMC.

You need to install this tool on a remote machine (for example, on a PC). You need to have a network connection from the remote machine to the BMC.

Downloaded from Arrow.com.

You can run the following command to determine the revisions:

```
./ipmitool –I lan –H 192.168.201.9 –U admin –P admin hpm check
```

7.5.2 Upgrade Procedure

This section describes the step-by-step procedure to upgrade firmware images on a MaxCore MC3000 prototype.

Procedure

To upgrade the firmware elements, perform the following steps:

1. **Upgrade the BMC Firmware**
   The BMC firmware should always be the first element to be upgraded. You can skip this step, if the BMC firmware already has the latest version.

   You can upgrade the BMC firmware through the BMC's web browser accessed from the remote machine (network connection from remote machine to BMC required) through the IP address *192.168.201.9* with *Username* **`admin`** and *Password* **`admin`**

NOTICE

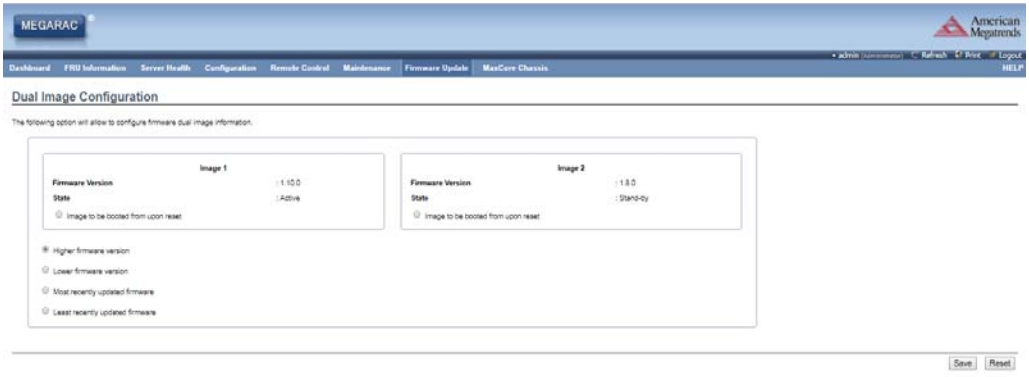
Firmware upgrades via web browser are only supported by firmware revisions higher than v1.0.10 (the BMC firmware revision can be retrieved with *ipmitool*, refer to *Obtaining Revisions of Firmware Components* on page 228).
In case the BMC firmware revision installed does not support upgrades via the web browser, the BMC FW EEPROM needs to be extracted from its socket on the MaxCore backplane and needs to be reprogrammed with a flasher hardware device (this option is required for very first prototypes only).

   BMC firmware revisions higher or equal to version 1.5.0 support two firmware images (active and inactive) to be maintained.

Downloaded from Arrow.com.

To view more details, open the **Dual Image Configuration** screen by clicking **Firmware Update** > **Dual Image Configuration**.

Figure 7-42 Dual Image Configuration

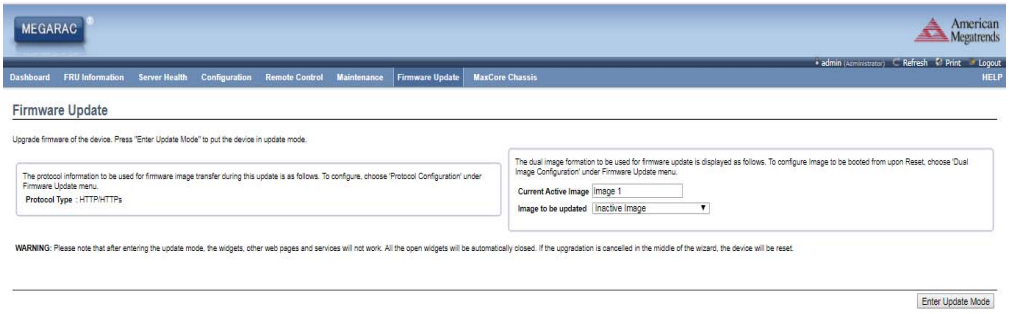


In the **Dual Image Configuration** screen, choose the required *Image* (that need to be booted after firmware option upgrade) and click **Save**.

Downloaded from Arrow.com.

To open **Firmware Update** screen, click **Firmware Update** > **Firmware Update** from menu bar.

Figure 7-43 Firmware Update - Upgrade



Do not modify the image to be updated. Never update the image you have booted successfully from.

- Select **Preserve Configuration** to preserve the network configuration (IP, username, password, DHCP, VLAN).

  For more details, refer to the section *Firmware Update* on page 188.

- Click **Enter Update Mode** and follow the wizard through the upgrade. Select **Full Flash** check box to perform a complete firmware upgrade always.

2. **Upgrade the Companion CPLD**

   You can skip this step, if the Companion CPLD firmware already has the most recent version. For more information, refer to *MaxCore MC3000 Release Notes*.
   Use the following command to upgrade the IO-CPLD.

Downloaded from Arrow.com.

```
./ipmitool –I lan –H 192.168.201.9 –U admin –P admin hpm
upgrade mc3000-cpld-companion-0.2.6.hpm component 3 force
```

NOTICE

- **In any case, if you observe that the firmware upgrade fails, repeat the firmware upgrade procedure again.**
- **Firmware upgrade progress is not seen immediately. As the first step, the *ipmitool* loads the firmware image into the BMC. This may take some time (~30sec).**
  In the next step, the *ipmitool* states
  `Writing firmware: 100% completed. Please do not stop execution at this point, ipmitool is still working!`

  Wait until the following message appears "Firmware upgrade procedure successful" (~2min).

3. **Upgrade the Glue CPLD**
   You can skip this step, if the Glue CPLD firmware already has the most recent version.
   Use the following command to upgrade the Glue CPLD.

```
./ipmitool –I lan –H 192.168.201.9 –U admin –P admin hpm
upgrade mc3000-cpld-glue-0.3.0.hpm component 2 force
```

NOTICE

- **If you observe that the firmware upgrade fails, repeat the firmware upgrade procedure again.**
- **Firmware upgrade progress is not seen immediately. As the first step, the *ipmitool* loads the firmware image into the BMC. This may take some time (~2min).**
  In the next step, the *ipmitool* states "Writing firmware: 100% completed".
  Please do not stop execution at this point, ipmitool is still working!
  Wait until the following message appears "Firmware upgrade procedure successful" (~3min).

Downloaded from Arrow.com.

4. **Upgrade the IO-Module CPLD**
   You can skip this step, if you have already programmed the actual firmware.
   Use the following command to upgrade the IO-CPLD.
   `./ipmitool –I lan –H 192.168.201.9 –U admin –P admin hpm upgrade mc3000-cpld-iomod-0.4.0 component 4 force`

NOTICE

- **In any case, if you observe that the firmware upgrade fails, repeat the firmware upgrade procedure again.**
- **You cannot see the Firmware upgrade progress immediately. As the first step, the *ipmitool* loads the firmware image into the BMC. This may take some time (~2min). In the next step, the *ipmitool* states Writing firmware: 100% completed. Please do not stop execution at this point, *ipmitool* is still working!**
  Wait until the following message appears Firmware upgrade procedure successful (~3min).
- **The "IO-Module" CPLD on early MaxCore prototypes cannot be upgraded at all (even when the revision can be read). Any attempt will fail during programming immediately. The revision of the respective system module can be determined only by dismounting the device and evaluating the part number at the PCB (8406843P41A PCB REV A). Contact your local Artesyn executive, if the firmware upgrade on such a system becomes necessary.**
  Subsequent firmware upgrades can be performed much faster due to a change in the I2C controller implementation in the CPLDs.

5. Remove and reinsert power plug.

7.5.3 Troubleshooting

This section is provided in this chapter to assist you with troubleshooting.

Downloaded from Arrow.com.

7.5.3.1 CPLD FW Upgrade Failed

Do not switch off system power until "*ipmitool* prompts *Firmware upgrade procedure successful*" or "*Firmware upgrade procedure failed*" message. Upgrading the "IO-Module" CPLD may take very long (~25min).

In case when *ipmitool* reports "*Firmware upgrade procedure failed*" message, power cycle the system, and evaluate the firmware revision of the firmware component just programmed (for more details refer to *Obtaining Revisions of Firmware Components* on page 228, and if the revision programmed is not performed before, repeat the firmware upgrade procedure. If subsequent CPLD firmware upgrade fails, contact your local Artesyn executive.

7.5.3.2 BMC FW Upgrade Failed

In such a case, power cycle the system and repeat the firmware upgrade. If subsequent BMC firmware upgrade fails, contact your local Artesyn executive.

7.5.3.3 BMC Cannot Be Accessed Via IP address

In case the BMC is not accessible via its IP address anymore there is a possibility to set the BMC to its factory defaults by pressing the reset button at the IO module (the BMC will automatically reboot).

After the reboot, you can access the BMC via the IP*192.168.201.9, username* **admin** and *password* **admin**. The DHCP will be in **Off** mode.

7.6 Modifying the BMC IP Address

The IP Address of the BMC can be modified either via web browser or via Linux tool called *ipmitool* executed at the mCPU. While modifying BMC IP address via browser refer to *Network* on page 144 and select LAN Interface eth1 in the network settings before modifying the IP address as per your requirement.

The following command is used to retrieve network specific information:

```
root@pcie7410_s_1_c_1: ipmitool -U admin -P admin lan print 1

Set in Progress: Set Complete

Auth Type Support: MD5
```


Downloaded from Arrow.com.

```
Auth Type Enable: Callback: MD5
                          : User     : MD5
                          : Operator : MD5
                          : Admin    : MD5
                          : OEM      : MD5
IP Address Source         : Static Address
IP Address                : 192.168.201.9
Subnet Mask               : 255.255.255.0
MAC Address               : 00:80:42:65:cd:01
SNMP Community String     : AMI
IP Header              : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
BMC ARP Control           : ARP Responses Enabled, Gratuitous ARP
Disabled
Gratituous ARP Intrvl     : 0.0 seconds
Default Gateway IP        : 0.0.0.0
Default Gateway MAC       : 00:00:00:00:00:00
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
RMCP+ Cipher Suites       : 0,1,2,3,6,7,8,11,12,15,16,17
Cipher Suite Priv Max     : caaaaaaaaaaaXXX
                          :     X=Cipher Suite Unused
```


Downloaded from Arrow.com.

```
                                :      c=CALLBACK
                                :      u=USER
                                :      o=OPERATOR
                                :      a=ADMIN
                                :      O=OEM
```

The following command is used to set the IP address of the BMC to *192.168.201.10*

```
root@pcie7410_s_1_c_1: ipmitool -U admin -P admin lan set 1 ipaddr
192.168.201.10

Setting LAN IP Address to 192.168.201.10
```



***ipmitool* does not return properly, if IP address is changed at the BMC.**

Downloaded from Arrow.com.

The mCPU is responsible for configuring the PLX PCIe bridges at the MC3000 system. Due to various use cases of this system, you may need to reconfigure the PLX PCIe bridges differently from that of the original ones provided by Artesyn.

If the you accidentally misconfigure the PLX PCIe bridges (for example, configuring a downstream port to host mode), a PCIe card may hang in BIOS trying to enumerate its PCIe buses endlessly. In case the mCPU is still booting up, the MCCS service can reconfigure the PLX PCIe bridges again. However, if the mCPU does not comes up, there would be no possibility to reconfigure the PLX PCIe bridges anymore.

In order to recover from this locking scenario, a utility called `mcbmtool` is provided. With `mcbmtool` you can set the PLX PCIe bridges to default (factory) mode, in order to invoke the mCPU to boot up again.

`mcbmtool` is the MaxCore system's basic management tool and it is provided as an executable file in the BMC. Execute the following command to know the list of parameters supported.

```
# mcbmtool -h

Usage: mcbmtool [OPTION]...

MaxCore Basic Management Tool.

GENERAL OPTIONS:

 -p --plane=NUM  use plane with number NUM

 -c --cmd=CMD  execute the command CMD (see below)

 -m, --cfgmode=MODE use config mode MODE (see below)

 -n, --cfgname=NAME use config with name NAME


ADVANCED OPTIONS:

  -l, --logfile=FILE   use file FILE as logfile
[default='/var/log/mcbmtool']

 -r, --rmcp    use RMCP to connect to the BMC
```


Downloaded from Arrow.com.

```
-i, --ipaddr=IPADDR useIPaddressIPADDR[default='127.0.0.1']
 -v, --verbose      be more verbose in logfile
MISCELLANEOUS OPTIONS:
-V, --version print version information and exit
-h, --help   display this help and exit

SUPPORTED CONFIG MODES:
 static
 dynamic
SUPPORTED COMMANDS:
 list-cfg-names : list all config names
 dump-cfg   : dump specified config
 dump-cur-cfg  : dump current config
 verify-cfg  : verify specified config with current one
 write-cfg   : write specified config
  manage-cfg      : verify and if necessary write specified config
```

You can use this tool in the following way:

1. Evaluate which configurations are provided.
   #**mcbmtool –c list-cfg-names**
   dynamic config names:
   default
   _test1
   base1_mcpu_s1c1
   base1_mcpu_s1c2
   base1_mcpu_s15c1
   base1_mcpu_s15c2
   fab1_mcpu_s1c1

Downloaded from Arrow.com.

```
fab1_mcpu_s1c2
fab1_mcpu_s15c1
fab1_mcpu_s15c2
```

2. Program PLX configuration.
   #**mcbmtool –c manage-cfg base1_mcpu_s1c1**
3. Reset the mCPU (do not turn off payload power).

NOTICE

User may need to stop grub and modify the grub boot line to start Linux in single mode. Otherwise, the `mccs` may reconfigure the PLX PCIe bridge into their latest configuration (which did not work before).

Downloaded from Arrow.com.

Downloaded from Arrow.com.

B.1 Artesyn Embedded Technologies - Embedded Computing Documentation

The publications listed below are referenced in this manual. You can obtain electronic copies of Artesyn Embedded Technologies - Embedded Computing publications by contacting your local Artesyn sales office. For released products, you can also visit our Web site for the latest copies of our product documentation.

1. Go to www.artesyn.com/computing/support/product/technical-documentation.php.
2. Under **FILTER OPTIONS**, click the **Document types** drop-down list box to select the type of document you are looking for.
3. In the **Search** text box, type the product or document name and click **Filter**.

Table B-1 Artesyn Embedded Technologies - Embedded Computing Publications

Document Title	Publication Number
SSF for MaxCore™ MC3000 Platform XML Interface Guide	6806800T71
MaxCore™ MC3000 Platform Software Installation and Use	6806800U97
SSF for MaxCore™ MC3000 Platform CLI Guide	6806800T87
MaxCore™ MC3000 Platform AC Quick Start Guide	6806800T89
MaxCore™ MC3000 Platform Safety Notes Summary	6806800T90
SharpServer™ PCIE-7410 Safety Notes Summary	6806800T94
SharpServer™ PCIE-7410 Quick Start Guide	6806800T96
MaxCore™ MC3000 Rail Kit Installation Quick Start Guide	6806800U24

Downloaded from Arrow.com.

B.2 Related Specifications

For additional information, refer to the following table for related specifications. As an additional help, a source for the listed document is provided. Please note that, while these sources have been verified, the information is subject to change without notice.

Table B-2 Related Specifications

Document Title	Source
Peripheral Component Interconnect Special Interest Group (PCI-SIG) www.pcisig.com	
PCI Express Base Specification Revision 3.1	PCI-SIG
PCI Express Card Electromechanical Specification Revision 3.0	PICMG
PICMG 3.1 Revision 1.0 Specification Ethernet/Fibre Channel for AdvancedTCA Systems, January 2003	PICMG

Downloaded from Arrow.com.

Downloaded from Arrow.com.





Artesyn Embedded Technologies, Artesyn and the Artesyn Embedded Technologies logo are trademarks and service marks of Artesyn Embedded Technologies, Inc.
All other product or service names are the property of their respective owners.
© 2018 Artesyn Embedded Technologies, Inc.

Downloaded from Arrow.com.

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP