Copyright

© Copyright 1998-2010 American Megatrends, Inc.
All rights reserved.
American Megatrends, Inc.
5555 Oakbrook Parkway
Building 200
Norcross, GA 30093

This publication contains proprietary information which is protected by copyright. No part of this publication can be reproduced, transcribed, stored in a retrieval system, translated into any language or computer language, or transmitted in any form whatsoever without the prior written consent of the publisher, American Megatrends, Inc. American Megatrends, Inc. acknowledges the following trademarks.

Intel is a registered trademark of the Intel Corporation.

MS-DOS and Microsoft are registered trademarks of the Microsoft Corporation. Microsoft Windows is a trademark of the Microsoft Corporation.

IBM, AT, VGA, PS/2, and OS/2 are registered trademarks and XT and CGA are trademarks of the International Business Machines Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. American Megatrends, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.
## Revision History

<table>
<thead>
<tr>
<th>S.No</th>
<th>Author</th>
<th>Document Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Smitha Sreedharan</td>
<td>1.0</td>
<td>Aug 20, 2010</td>
<td>The document with the latest SPX features</td>
</tr>
<tr>
<td>2</td>
<td>Smitha Sreedharan</td>
<td>1.1</td>
<td>Aug 24, 2010</td>
<td>Included PEF, CIM</td>
</tr>
<tr>
<td>3</td>
<td>Smitha Sreedharan</td>
<td>1.2</td>
<td>Oct 19, 2010</td>
<td>vmedia related notes updated</td>
</tr>
<tr>
<td>4</td>
<td>Smitha Sreedharan</td>
<td>1.3</td>
<td>Oct 27, 2010</td>
<td>Added new topics - FRU Information, Local Media, NCSI, SNMP and Virtual Media. Updated VMedia and Keyboard Layouts.</td>
</tr>
<tr>
<td>5</td>
<td>Smitha Sreedharan</td>
<td>1.4</td>
<td>Nov 29, 2010</td>
<td>Updated PEF</td>
</tr>
</tbody>
</table>
# Table of Contents

Copyright ................................................................................................................................................................................................. 2
Revision History .............................................................................................................................................................................................. 3
Limited Warranty .............................................................................................................................................................................................. 7
Technical Support .......................................................................................................................................................................................... 8
Website ................................................................................................................................................................................................ 8
Disclaimer ................................................................................................................................................................................................. 9
Retail Packing List ....................................................................................................................................................................................... 10

## INTRODUCTION .................................................................................................................................................................................... 11

Notes ........................................................................................................................................................................................................... 11
Overview ............................................................................................................................................................................................. 12
Supported SoC and Hardware platforms ............................................................................................................................................... 13

## SP-X FEATURES ................................................................................................................................................................................ 14

IPMI Message Interface Support ................................................................................................................................................................. 14
Media Redirection ....................................................................................................................................................................................... 14
IPMI 2.0 based management .................................................................................................................................................................. 14
Event Log and Alerting ............................................................................................................................................................................ 14
Sophisticated User Management ............................................................................................................................................................ 14
LDAP support ............................................................................................................................................................................................ 15
Remote Server Power Control .................................................................................................................................................................. 15
Common Information Model (CIM) .......................................................................................................................................................... 15
SSH based SOL .......................................................................................................................................................................................... 15
WSMAN Support .......................................................................................................................................................................................... 15
Web based configuration .......................................................................................................................................................................... 16

## SP-X WEB GUI .................................................................................................................................................................................. 17

MegaRAC® GUI Overview ......................................................................................................................................................................... 17
Supported Browsers .................................................................................................................................................................................... 17
Supported OS ............................................................................................................................................................................................. 17
User Name and Password ......................................................................................................................................................................... 19
Default User Name and Password .......................................................................................................................................................... 21

## Using MegaRAC SP-X ........................................................................................................................................................................ 22

Menu Bar .................................................................................................................................................................................................... 22
Quick Button and Logged-in User .......................................................................................................................................................... 22

Dashboard .................................................................................................................................................................................................. 24

## FRU Information ................................................................................................................................................................................ 26

## Server Health Group .......................................................................................................................................................................... 28

Sensor Readings .......................................................................................................................................................................................... 29
## Configuration Group

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>36</td>
</tr>
<tr>
<td>DNS</td>
<td>40</td>
</tr>
<tr>
<td>LDAP</td>
<td>43</td>
</tr>
<tr>
<td>Local Media</td>
<td>46</td>
</tr>
<tr>
<td>Mouse Mode</td>
<td>48</td>
</tr>
<tr>
<td>NCSI</td>
<td>49</td>
</tr>
<tr>
<td>Network</td>
<td>50</td>
</tr>
<tr>
<td>NTP</td>
<td>52</td>
</tr>
<tr>
<td>PEF</td>
<td>54</td>
</tr>
<tr>
<td>RADIUS</td>
<td>64</td>
</tr>
<tr>
<td>Remote Session</td>
<td>67</td>
</tr>
<tr>
<td>SMTP</td>
<td>69</td>
</tr>
<tr>
<td>SNMP</td>
<td>72</td>
</tr>
<tr>
<td>SSL</td>
<td>74</td>
</tr>
<tr>
<td>System and Audit Log</td>
<td>76</td>
</tr>
<tr>
<td>User management</td>
<td>78</td>
</tr>
<tr>
<td>Virtual Media</td>
<td>81</td>
</tr>
</tbody>
</table>

## Remote Control

<table>
<thead>
<tr>
<th>Remote Control</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console Redirection</td>
<td>84</td>
</tr>
<tr>
<td>Console Redirection Menu</td>
<td>86</td>
</tr>
<tr>
<td>Video</td>
<td>86</td>
</tr>
<tr>
<td>Keyboard</td>
<td>87</td>
</tr>
<tr>
<td>Mouse</td>
<td>88</td>
</tr>
<tr>
<td>Options</td>
<td>89</td>
</tr>
<tr>
<td>Media</td>
<td>90</td>
</tr>
<tr>
<td>Keyboard Layout</td>
<td>92</td>
</tr>
<tr>
<td>Video Record</td>
<td>93</td>
</tr>
<tr>
<td>Help</td>
<td>94</td>
</tr>
<tr>
<td>Quick Buttons</td>
<td>95</td>
</tr>
<tr>
<td>Server Power Control</td>
<td>96</td>
</tr>
</tbody>
</table>

## Maintenance Group

<table>
<thead>
<tr>
<th>Maintenance Group</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Update</td>
<td>97</td>
</tr>
<tr>
<td>Restore Factory Defaults</td>
<td>98</td>
</tr>
</tbody>
</table>

## LOG OUT

LOG OUT ................................................................. 99

## FLASH TOOLS

FLASH TOOLS ............................................................ 100

YAFUFlash: ............................................................... 100
Limited Warranty

The buyer agrees that if this product proves to be defective, American Megatrends is only obligated to repair or replace this product at American Megatrends’ discretion according to the terms and conditions of the warranty registration card that accompanies this product. American Megatrends shall not be liable in tort or contract for any loss or damage, direct, incidental or consequential resulting from the use of this product. Please see the Warranty Registration Card shipped with this product for full warranty details.
Technical Support

AMI provides technical support for AMI products purchased directly from AMI or from an AMI-authorized reseller only.

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You purchased this product from AMI or from a certified AMI reseller,</td>
<td>Call AMI technical support at 770-246-8645. Please be prepared to specify the serial number of the product.</td>
</tr>
<tr>
<td>This AMI product was installed as part of a system manufactured by a company other than AMI or you purchased an AMI product from an unauthorized reseller.</td>
<td>Call the technical support department of the computer manufacturer or the unauthorized reseller. AMI does not provide direct technical support in this case.</td>
</tr>
</tbody>
</table>

If an American Megatrends MegaRAC® SP-X fails to operate as described or you are in doubt about a configuration option, please call technical support at 770-246-8645.

Website

We invite you to access the American Megatrends World Wide Website at:

http://www.ami.com/
Disclaimer

This manual describes the operation of the American Megatrends’ MegaRAC® SP-X firmware. SoC board (Server Engines’ reference platform for SoC) was used to validate the functionality. Although efforts have been made to assure the accuracy of the information contained here, American Megatrends expressly disclaims liability for any error in this information, and for damages, whether direct, indirect, special, exemplary, consequential or otherwise, that may result from such error, including but not limited to the loss of profits resulting from the use or misuse of the manual or information contained therein (even if American Megatrends has been advised of the possibility of such damages). Any questions or comments regarding this document or its contents should be addressed to American Megatrends at the address shown on the inside of the front cover.

American Megatrends provides this publication “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a specific purpose.

Some states do not allow disclaimer of express or implied warranties or the limitation or exclusion of liability for indirect, special, exemplary, incidental or consequential damages in certain transactions; therefore, this statement may not apply to you. Also, you may have other rights which vary from jurisdiction to jurisdiction.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. American Megatrends may make improvements and/or revisions in the product(s) and/or the program(s) described in this publication at any time.

Requests for technical information about American Megatrends products should be made to your American Megatrends authorized reseller or marketing representative.
Retail Packing List

You must have received the following:

A motherboard with SoC and MegaRAC® SP-X on SoC installed
MegaRAC® SP-X User Guide
MegaRAC® SP-X CD
Introduction

Notes

This document describes the engineering specifications for the features of the new core (SP-X) of AMI’s generic MegaRAC® SP firmware. This document, until and unless specified, confirms the functionality on all the SoC platforms listed in this document.

“Generic MegaRAC® SP-X core” refers to the new core of AMI’s MegaRAC® SP firmware running on various SoC platforms.

“SP” and “Service Processor” terms are used interchangeably throughout this document to refer to AMI’s generic MegaRAC® SP solution.

“MegaRAC® SP-X”, “MegaRAC SP”, “SP-X”, “SP-X Core” and “Generic MegaRAC® SP” terms are used interchangeably throughout this document to refer to AMI’s service processor firmware solution.

Any or all CIM based SMASH/WSMAN or SMASH-Lite functionality mentioned in this document may or may not be available in all versions of Generic MegaRAC® SP. Please refer to the release notes of your firmware version for more details.

Although this document explains the new features etc of the new MegaRAC SP core, it also includes specific details about the existing core (core 2.0), whenever necessary. The sections where core 2.0 is mentioned are: supported SoC platforms and schedule/release milestones.
Overview

Generic MegaRAC® SP is a powerful software stack combining the functionality of a Service Processor and of a Baseboard Management Controller (BMC). The software implements IPMI 2.0 and KVM/IP based on the service processor. It performs all the BMC management tasks defined by IPMI 2.0 and, as a Service Processor, allows for video redirection and remote monitoring using KVM over LAN or Serial over LAN. For remote access, MegaRAC-SP runs an embedded web-server, provides a command line interface according to the DMTF SMASH specification, and WSMAN support. MegaRAC® SP also provides Secure-Shell (SSH) based SOL to provide remote access. MegaRAC® SP is also available for all the advanced System-On-Chips (SoC) on the market today. AMI currently has partnerships with many of today’s leading SoC silicon suppliers.

MegaRAC® SP can be completely customized and enriched with MegaRAC® DS, an Integrated Development Environment (IDE), for server management designed as a set of Eclipse Plug-ins (www.eclipse.org).

The new core (SP-X) of MegaRAC® firmware provides higher level of modularity in the stack, ability to easily configure the complete stack by selecting/selecting features which are now available in the packages form. There are various other improvements like new Linux kernel base, new set of automated test tools, and easy portability/customization using supplied tools. MegaRAC® DS has been extended to include the ability to customize the stack, build and debug at the same time.
**Supported SoC and Hardware platforms**

This section lists out the supported SoC platforms by MegaRAC SP-X core. It also includes the SoC platforms on which the existing MegaRAC SP core 2.0 has been officially released.

<table>
<thead>
<tr>
<th>SoC vendor</th>
<th>SoC/EVB</th>
<th>Core 2.0</th>
<th>SP-X Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Engines</td>
<td>Pilot-II/Aviator</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server Engines</td>
<td>Pilot-III/Hornet</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Renesas</td>
<td>Rainier (SH7757)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Winbond</td>
<td>Hermon(WPCM450)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Nuvoton</td>
<td>Yarkon</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Maxim</td>
<td>VSC452</td>
<td>No</td>
<td>TBD</td>
</tr>
<tr>
<td>Aspeed</td>
<td>AST2050</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Aspeed</td>
<td>AST2100</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The hardware platform used to validate MegaRAC SP stack typically is:

The SoC EVB plugged-in to AMI’s Olympus (876) motherboard or any other motherboard, required by the SoC EVB.

In addition, an I2C board and another BMC are used to validate I2C related functionality of MegaRAC SP core. This setup is being added to ensure that generic releases of MegaRAC SP core includes actual, real-time sensors/server health management, FRU, and multi-master functionality. Please refer to the later sections of this document for more details on this I2C setup.
SP-X Features

IPMI Message Interface Support

- KCS (System Interface Support)
- IPMB
- LAN
- USB

Media Redirection

- Simultaneous floppy, Hard disk or USB and CD or DVD redirection.
- Efficient USB 2.0 based CD/DVD redirection with a typical speed of 20XCD.
- Support for USB key
- Completely secured (Authenticated or Encrypted) remote KVM or vMedia.

IPMI 2.0 based management

- BMC stack with a full IPMI 2.0 implementation
- Customizable sensor management

Event Log and Alerting

- Read Log events
- Sensor readings
- SNMP traps
- E-Mail alerts

Sophisticated User Management

- IPMI based user management
- Added security with SSL (HTTPS)
- Multiple user permission level
- Multiple user profiles
LDAP support

- Direct LDAP support from the device
- Open LDAP (Generic LDAP) supported

Remote Server Power Control

- Server’s power status report
- Support for remotely power-cycle, power-down, power-up and reset the server

Common Information Model (CIM)

- CIM Object Manager (CIMOM)
- True Object Manager with CIM class handling
- Creating class, instance and working with the instances
- Core support for all DMTF profiles
- Extendible for additional OEM profiles
- SMASH and CLP support

SSH based SOL

- Power control of the server
- Support for all DMTF Profiles
- Complete command support
- Customizable parser for easy update to future modifications in grammar
- Dynamic target discovery
- Firmware update
- Role based authentication and authorization
- Output filtering
- Configurable profile mapping. (CIM Methods to SMASHCLP command mapping)
- OEM command and target

WSMAN Support

- Supports WSMAN as well as WS-CIM
- Rich SDK capability for OEM extensions
• Organically fully developed code as library
• Can work with any web server
• Currently supported web server- GoAhead
• HTTP and HTTPS support
• Complete WSMAN support – Discovery, Enumeration, Get, Put, Subscribe and gather Events.
• Rich client library support (C, Java, JavaScript)

**Web based configuration**

• Full configuration using web UI
• Fail-safe firmware upgrade
• Multi-language support in Web interface with English as the currently supported language
MegaRAC® GUI Overview

The MegaRAC® SP-X on SoC has an AMI generic, user-friendly Graphics User Interface (GUI) called the MegaRAC® GUI. It is designed to be easy to use. It has a low learning curve because it uses standard Internet browsers.

This chapter allows you to become familiar with the MegaRAC® GUI’s various functions. Each function is described in detail.

Note: Your MegaRAC® GUI may not exactly match this document.

Supported Browsers

- Internet Explorer 7 and above
- Firefox 2.0 and above
- Google Chrome 2.0 and above
- Safari 3.0 and above
- Opera 9.64 and above

Supported OS

- Windows XP
- Windows Vista
- w2k3 - 32 bit
- w2k3 - 64 bit
- RHEL 4 - 32 bit
- RHEL 4 - 64 bit
- RHEL 5.4 - 32 bit
- RHEL 5.4 - 64 bit
- Ubuntu 9.10 LTS – 32
- Ubuntu 9.10 LTS – 64
- Ubuntu 8.10 -32
- Ubuntu 8.10 -64
- OpenSuse 11.2 -32
- OpenSuse 11.2 -64
- FC 9 – 32 and above
- FC 9 – 64 and above
- MAC -32
- MAC-64
User Name and Password

Initial access of MegaRAC SP-X prompts you to enter the User Name and Password. A screenshot of the login screen is given below.

The fields are explained as follows:

**Username**

Enter your username in this field.

**Password**

Enter your password in this field.

**Login**

After entering the required credentials, click the button to login to MegaRAC GUI.

**Forgot Password**

If you forget your password, you can generate a new one using this link.
Enter the username, click on **Forgot Password** link. This will send the newly generated password to the configured Email-ID for the user.

**Allow popups from this site**

The icon indicates whether the browser allows popup for this site or not.

**Allow file download from this site**

For Internet Explorer, Choose **Tools ->Internet Options ->Security Tab**, based on device setup, select among Internet, Local intranet, trusted sites and restricted sites. Click **Custom level...**. In the Security Settings - Zone dialog opened, under settings, find Downloads option, Enable File download option. Click **OK** to the entire dialog boxes.

For all Other Browsers, accept file download when prompted.

**Enable javascript for this site**

The icon indicates whether the javascript setting is enabled in browser.

**Enable cookies for this site**

The icon indicates whether the cookies setting are enabled in browser.

**NOTE:** Cookies must be enabled in order to access the website.
Default User Name and Password

The default user name and password are as follows:

**Username:** root

**Password:** superuser

**Note:**
- The default user name and password are in lower-case characters.
- When you log in using the root user name and password, you get full administrative rights. It is advised to change your password once you login.
Using MegaRAC SP-X

The MegaRAC GUI consists of various menu items.

Menu Bar

The top menu bar displays the following.

- Dashboard
- Server Health
- Configuration
- Remote Control
- Maintenance

A screenshot is of the top menu bar is given below.

```
Dashboard | Server Health | Configuration | Remote Control | Maintenance
```

Top Menu Bar

Quick Button andLogged-in User

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

User Information

The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allows you to perform the following functions.
Logged-in user and its privilege level

This option shows the logged-in user name and privilege. There are five kinds of privileges.

- **User**: Only benign 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**

Click the [Refresh] icon to reload the current page.

**Print**

Click the [Print] icon to take the print out of the current page.

**Logout**

Click the [Logout] icon to log out of the MegaRAC® GUI.

**HELP**

Click [HELP] to view the help page.
Dashboard

In MegaRAC GUI, the Dashboard page gives the overall information about the status of a device.

To open the Dashboard page, click **Dashboard** from the main menu. A sample screenshot of the Dashboard page is shown below.
Given below is a brief description about the various informations displayed in the Dashboard page.

**Device Information**

The Device Information displays the following informations.

- **Device Power Status**: This field shows if the power of the device is on or off.
- **Firmware Revision**: The revision number of the firmware.
- **Firmware Build Time**: This field shows the date and time on which the firmware is built.

**Network Information**

The Network Information of the device with the following fields is shown here. To edit the network Information, click **Edit**.

- **MAC Address**: Read only field showing the IP address of the device.
- **V4 Network Mode**: The v4 network mode of the device which could be either disable, static or DHCP.
- **IPv4 Address**: The static IPv4 address.
- **V6 Network Mode**: The v6 network mode of the device which could be either disable, static or DHCP.

**Remote Control**

To redirect the host remotely, launch Java Console or ActiveX Console from this section. There are two types of consoles related.

- **Java Console**: Click Launch to launch the console redirection and to manage the remote server. This downloads the jviewer.jnlp file which after downloaded and launched will open the Java redirection window.
- **ActiveX Console**: Click Launch to download the ActiveX Control, install it and launch the ActiveX redirection window.

Detailed descriptions of these consoles are given in **Remote Control > Console Redirection**.

**Sensor Monitoring**

It lists all the available sensors on the device with the following information’s.

- **Status**: The status column displays the state of the device. There are three states.
  - ○ - Denotes normal state
  - ⚠ - Denotes Warning State
  - ☠ - Denotes Critical State

If you click the ⚡ icon, the sensor page for that particular sensor will be displayed.
**FRU Information**

In MegaRAC GUI, the FRU Information Page displays the BMC FRU file information. The information displayed in this page are Basic Information, Common Header Information, Chassis Information, Board Information and Product Information of the FRU device.

To open the FRU Information Page, click **FRU Information** from the top menu. Select a FRU Device ID from the Basic Information section to view the details of the selected device. A screenshot of FRU Information page is given below.

![FRU Information Page](image)

The following fields are displayed here for the selected device.

<table>
<thead>
<tr>
<th>Field Replaceable Unit (FRU)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Information:</strong></td>
<td></td>
</tr>
<tr>
<td>FRU Device ID</td>
<td>0</td>
</tr>
<tr>
<td>FRU Device Name</td>
<td>BMC_FRU</td>
</tr>
<tr>
<td><strong>Chassis Information:</strong></td>
<td></td>
</tr>
<tr>
<td>Chassis Information Area Format Version</td>
<td>1</td>
</tr>
<tr>
<td>Chassis Type</td>
<td>Ptera Box</td>
</tr>
<tr>
<td>Chassis Part Number</td>
<td>7058BE4</td>
</tr>
<tr>
<td>Chassis Serial Number</td>
<td>A094-035</td>
</tr>
<tr>
<td>Custom Fields</td>
<td>AME</td>
</tr>
<tr>
<td><strong>Board Information:</strong></td>
<td></td>
</tr>
<tr>
<td>Board Information Area Format Version</td>
<td>1</td>
</tr>
<tr>
<td>Language</td>
<td>0</td>
</tr>
<tr>
<td>Manufacture Date/Time</td>
<td>Sun Oct 3 22:38:00 2010</td>
</tr>
<tr>
<td>Board Manufacturer</td>
<td>AME</td>
</tr>
<tr>
<td>Board Product Name</td>
<td>AME</td>
</tr>
<tr>
<td>Board Serial Number</td>
<td>00001</td>
</tr>
<tr>
<td>Board Part Number</td>
<td>00001</td>
</tr>
<tr>
<td>FRU File ID</td>
<td></td>
</tr>
<tr>
<td>Custom Fields</td>
<td>AME</td>
</tr>
<tr>
<td><strong>Product Information:</strong></td>
<td></td>
</tr>
<tr>
<td>Product Information Area Format Version</td>
<td>1</td>
</tr>
<tr>
<td>Language</td>
<td>0</td>
</tr>
<tr>
<td>Manufacturer Name</td>
<td>AME</td>
</tr>
<tr>
<td>Product Name</td>
<td>AME</td>
</tr>
<tr>
<td>Product Part Number</td>
<td>1414B25</td>
</tr>
<tr>
<td>Product Version</td>
<td>3.3</td>
</tr>
<tr>
<td>Product Serial Number</td>
<td>12578578</td>
</tr>
<tr>
<td>Asset Tag</td>
<td>23423</td>
</tr>
<tr>
<td>FRU File ID</td>
<td></td>
</tr>
<tr>
<td>Custom Fields</td>
<td>AME</td>
</tr>
</tbody>
</table>
Basic Information
• FRU device ID - Select the device ID from the drop down list
• Device Name - The device name of the selected FRU device.

Chassis Information
• Area Format Version
• Chassis Type
• Chassis Part Number
• Chassis Serial Number
• Custom Fields

Board Information
• Area Format Version
• Language
• Manufacture Date Time
• Board Manufacturer
• Board Product Name
• Board Serial Number
• Board Part Number
• FRU File ID
• Custom Fields

Product Information
• Area Format Version
• Language
• Manufacturer Name
• Product Name
• Product Part Number
• Product Version
• Product Serial Number
• Asset Tag
• FRU File ID
• Custom Fields
Server Health Group

The Server Health Group consists of three items.

- Sensor Readings
- Event Log
- System and Audio Log

The screenshot displaying the menu items under Server Health is shown below.

![Server Health – Menu](image-url)
Sensor Readings

In MegaRAC GUI, the Sensor readings Page displays all the sensor related information.

To open the Sensor readings page, click **Server Health > Sensor Readings** from the top menu. Click on a record to show more information about that particular sensor, including thresholds and a graphical representation of all associated events. A screenshot of Sensor Readings page is given below.

Sensor Readings Page
The Sensor Readings page contains the following information.

**Sensor Type (drop down menu)**

This drop down menu allows you to select the type of sensor. The List of sensors with the Sensor Name, Status and Current Reading will be displayed in the list. If you select All Sensors, all the available sensor details will appear else you can choose the sensor type that you want to display in the list. Some examples of other sensors include Temperature Sensors, Fan Sensors, and Voltage Sensors etc.

Select a particular sensor from the list. On the right hand side of the screen you can view the Thresholds for this 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)


A graphical view of these events (Number of event logs vs. Thresholds) can be viewed as shown in the Sensor Readings Page screenshot.
**Live Widget**

For the selected sensor, you can click ON or OFF to turn the widget paper or disappear. This widget gives a dynamic representation of the readings for the sensor. Given below is a sample screenshot when the widget is on.

![CPU 2 Voltage](image)

**Note:** Widgets are little gadgets, which provide real time information about a particular sensor. User 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 gets a live data of the last widget that is kept opened.

**View this Event Log**

You can click here to view the Event Log page for the selected sensor.
Event Log

In MegaRAC GUI, this page 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.

To open the Event Log page, click **Server Health > Event Log** from the top menu. A sample screenshot of Event Log page is shown below.
The Event Log page consists of the following Fields.

**Event log Category**

From the drop down menu, select the event categories. The category could be either Sensor-Specific Event, BIOS Generated event or System Management Software event.

**Filter Type**

From the dropdown list, select the sensor name filer to view the event for the selected filer.

**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

**Clear All Event**

Click this option to delete all the existing records for all the sensors.
System & Audit logs

In MegaRAC GUI, if configured, these logs will display all the system and audit events that occurred in this device.

To open the Event Log page, click **Server Health > System and Audit Log** from the top menu.

**NOTE:** Logs have to be configured under 'Configuration -> System and Audit Log' in order to display any entries.

A sample screenshot of System and Audit Log page is shown below.

![System and Audit Log](image)

**System Log**

Click the System Log tab to view all system events. Entries can be filtered based on their levels like Alert, Critical, Error, Notification, Warning, Debug, Emergency and Information.

**Audit Log**

Click the Audit Log tab to view all audit events for this device.
Configuration Group

This group of pages allows you to access various configuration settings. A detailed description of each configuration group is given ahead. A screenshot of Configuration Group menu is shown below.

![Configuration Group Menu](image)

A detailed description of the Configuration menu is given ahead.
**Active Directory**

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. An active directory (sometimes referred to as an AD) does a variety of functions including the ability to provide information on objects, helps organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory.

This page in MegaRAC SP-X, allows you to Configure Active Directory Server Settings.

To open Active Directory Settings page, click **Configuration > Active Directory** from the main menu. A sample screenshot of Active Directory Settings Page is shown in the screenshot below.

![Active Directory Settings Page](image-url)
The fields of Active Directory Page are explained below.

**Advanced Settings:**

This option is used to configure Active Directory Advanced Settings. Options are Enable Active Directory Authentication, User Domain name, Time Out and up to three Domain Controller Server Addresses.

**Role Group ID:** The name that identifies the role group in the Active Directory.

Note:
- Role Group Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen and underscore are allowed.

**Role Group Name:** The domain where the role group is located.

Note:
- Domain Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen, underscore and dot are allowed.

**Role Group Privilege:** The level of privilege to assign to this role group.

**Add Role Group:** To add a new role group to the device.

**Modify role Group:** To modify that role group. Alternatively, double click on the configured slot.

**Delete Role Group:** To delete an existing Role Group.
**Procedure**

**Entering the details in Advanced Active Directory Settings Page**

1. Click on **Advanced Settings** to open the Advanced Active Directory Settings Page.

2. In the Active Directory Settings Page, enter the following details.

3. **Active Directory Authentication**: To enable/disable Active Directory, check or uncheck the **Enable** checkbox respectively.

   Note:
   If you have enabled Active Directory Authentication, enter the required information to access the Active Directory server.

4. Specify the Domain Name for the user in the **User Domain Name** field. e.g. MyDomain.com

5. Specify the time (in seconds) to wait for Active Directory queries to complete in the **Time Out** field.

   Note:
   - Default Time out value: 120 seconds.
   - Range from 15 to 300 allowed.

6. Configure IP addresses in **Domain Controller Server Address1**, **Domain Controller Server Address2** & **Domain Controller Server Address3**

   Note:
   IP address of Active Directory server: At least one Domain Controller Server Address must be configured.
   - 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.

7. Click **Save** to save the entered settings and return to Active Directory Settings Page.

8. Click **Cancel** to cancel the entry and return to Active Directory Settings Page.
To add a new Role Group

9. In the Active Directory Settings Page, select a blank row and click **Add Role Group** to open the Add Role group Page as shown in the screenshot below.

![Add Role Group Page](image)

10. In the **Role Group Name** field, enter the name that identifies the role group in the Active Directory.
    
    Note:
    
    - Role Group Name is a string of 255 alpha-numeric characters.
    - Special symbols hyphen and underscore are allowed.

11. In the **Role Group Domain** field, enter the domain where the role group is located.
    
    Note:
    
    - Domain Name is a string of 255 alpha-numeric characters.
    - Special symbols hyphen, underscore and dot are allowed.

12. In the **Role Group Privilege** field, enter the level of privilege to assign to this role group.

13. Click **Add** to save the new role group and return to the Role Group List.

14. Click **Cancel** to cancel the settings and return to the Role Group List.

To Modify Role Group

15. In the Advanced Directory Settings Page, select the row that you wish to modify and click **Modify Role Group**.

16. Make the necessary changes and click **Save**.

To Delete a Role Group

17. In the Advanced Directory Settings Page, select the row that you wish to delete and click **Delete Role Group**.
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 various informations 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.

In MegaRAC GUI, the DNS Server settings page is used to manage the DNS settings of a device.

To open DNS Server Settings page, click **Configuration > DNS** from the main menu. A sample screenshot of DNS Server Settings Page is shown in the screenshot below.

![DNS Server Settings Page](image-url)
The fields of DNS Server Settings page are explained below.

**Host configuration**

- **Host Settings**: Choose either Automatic or Manual settings.
- **Host Name**: It displays hostname of the device. If the Host setting is chosen as Manual, then specify the hostname of the device.

**Register BMC**

- **LAN Interface**: To define or not define the LAN Interface. If this flag is enabled for particular interface, then that interface will be registered with the DNS server.

**Domain Name Configuration**

- **Domain Settings**: It lists the option for domain interface as Manual, v4 or v6 for multiLAN channels.
  
  Note: If you choose DHCP, then select v4 or v6 for DHCP servers.

- **Domain Name**: It displays the domain name of the device. If the Domain setting is chosen as Manual, then 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.

**IPv4 Domain Name Server Configuration**

- **DNS Server Settings**: It lists the option for v4 DNS settings for the device, Manual and available LAN interfaces.

- **Preferred DNS Server**: The DNS (Domain Name System) server v4 address to be configured to the device.
  
  - 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.

- **Alternate DNS Server**

**IPv6 Domain Name Server Configuration**

- **DNS Server Settings**: It lists the option for v6 DNS settings for the device, Manual and available LAN interfaces. If you choose Manual setting, you have to configure the DNS Server Ip addresses. If you have chosen DHCP, then you have to select the interface from which the IP address is to be received. Example of IPv6 address - 2001:db8:0::101

- **Preferred DNS Server, Alternate DNS Server**: Specify the DNS (Domain Name System) server v6 address to be configured to the device.

**Save**: To save the entered changes.
**Reset:** To reset the entered changes.

**Procedure**

1. 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.
2. Enter the **Host Name** in the given field if you have chosen Manual Configuration.
3. In the **Domain name Configuration Settings**, select the domain settings from the dropdown list.
4. Enter the **Domain Name** in the given field

**IPv4 Domain Name Configuration,**

5. Select the **DNS Server Settings**, from the dropdown list
6. In the **Preferred DNS Server** field, enter the preferred IP address.
7. In the **Alternate DNS Server** field, enter the alternate address.
8. Click **Save** to save the entries.
9. Click **Reset** to reset the entries.
LDAP

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

In MegaRAC GUI, LDAP is an Internet protocol that MegaRAC card can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate MegaRAC card users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the MegaRAC card. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group-based policies to control access.

To open LDAP Settings page, click Configuration > LDAP from the main menu. A sample screenshot of LDAP Settings Page is shown in the screenshot below.

LDAP Settings Page
The fields of LDAP Authentication Page are explained below.

**LDAP Authentication**: To enable or disable LDAP authentication.

**Port**: The LDAP Port.

- **NOTE:**
  - Default Port is 389. For Secure connection, default port is 636.

**IP Address**: The IP Address of your LDAP Server in this field.

- **NOTE:**
  - IP Address is 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.

**Search base**: The Search base tells the LDAP server which part of the external directory tree to search. The search base may be something equivalent to the organization, group or external directory.

- **NOTE:**
  - Searchbase is a string of 4 to 63 alpha-numeric characters.
  - It must start with an alphabetical character.
  - Special Symbols like dot(,), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
  - Example: dc=domain,dc=com

**Bind DN**: The Bind DN in this field. The Bind DN (distinguished name) is the user on the LDAP server that is permitted to search the LDAP directory within the defined search base.

- **NOTE:**
  - Bind DN is a string of 4 to 63 alpha-numeric characters.
  - It must starts with an alphabetical character.
  - Special Symbols like dot(,), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
  - Example: cn=root,dc=domain,dc=com

**Bind Password**: The Authentication password for LDAP server

- **NOTE:**
  - Password must be at least 4 characters long.
  - White space is not allowed.
  - This field will not allow more than 31 characters.
**Save:** To Save to save the entered settings.

**Reset:** To Reset to reset the modified changes.

**Procedure**

1. Check the option **Enable** to enable the LDAP Authentication.
2. In the **LDAP** field, specify the LDAP Port.
3. On the **LDAP Server** field, enter the IP Address of the LDAP Server.
4. In the **Search Base** field, enter the Search Base.
5. In the **Blind DN** field, enter the Blind Distinguished Name.
6. In the **Blind Password** field, enter the password.
7. Click **Save** to save the entries.
8. Click **Reset** to reset the entries.
Local Media

In MegaRAC GUI, this page 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 **Configuration -> Virtual Media**. Once you enable this option, the host displays the devices enabled by Local Media and Virtual Media.

**Note:**
- To replace or add an image, you must have Administrator Privileges.
- Only one image can be uploaded for each image type. If the existing image and uploading image name is same, then a message is shown “Image already exists”.
- In Local Media redirection, the maximum upload size is 8MB.
**Procedure:**

The following actions can be performed in this page

**Add Image**

Select a free slot and click **Add Image** to upload a new image to the device. Alternatively, double click on a free slot to add an image. A sample screenshot of Add Image screen is given below.

![Add Image Screen](image)

**Replace Image**

Select a configured slot and click **Replace Image** to replace the existing image. Alternatively, double click on the configured slot.

Browse the image File and click **Replace**

**Delete Image**

Select a record and click **Delete Image** to delete the selected image.
Mouse Mode

In MegaRAC GUI, Redirection Console handles mouse emulation from local window to remote screen in either of two methods. User has to be an Administrator to configure this option.

To open Mouse Mode page, click **Configuration > Mouse Mode** from the main menu. A sample screenshot of Mouse Mode Settings Page is shown in the screenshot below.

![Mouse Mode Settings Page](image)

The fields of Mouse Mode Settings page are explained below.

**Absolute Mode:** The absolute position of the local mouse is sent to the server.

**Relative Mode:** Relative mode sends the calculated relative mouse position displacement to the server.

**Save:** To save any changes made.

**Reset:** To Reset the modified changes.

**Procedure**

1. Choose either of the following as your requirement:
   - **Set mode to Absolute**
   - **Set mode to Relative radio**
2. Click **Save** button to save the changes made.
3. Click **Reset** to reset the modified changes.
NCSI

In MegaRAC GUI, this page is used to configure Network Communication Service Interface (NCSI) configuration settings.

To open NCSI page, click **Configuration > NCSI** from the main menu. A sample screenshot of NCSI Page is shown in the screenshot below.

![NCSI Page Screenshot](image)

**Configure NCSI**

The following fields are displayed in this page

**Interface Name:** It 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**

1. Choose the particular **Interface Name** 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.
**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 main menu. A sample screenshot of Network Settings Page is shown in the screenshot below.

![Network Settings Page](image)

The fields of Network Settings page are explained below.

**MAC Address:**

This field displays the MAC Address of the device. This is a read only field.

**IPv4 Settings:** This option lists the IPv4 configuration settings

- Obtain IP Address automatically: This option is 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 Settings:** This option lists the following IPv6 configuration settings.

**IPv6 Settings:** This option is to enable the IPv6 settings in the device.

**Obtain an IPv6 address automatically:** This option is 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. Eg: 2004::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.

**Save:** To save the entries.

**Reset:** Reset the modified changes.

**Procedure**

1. In IPv4 Settings, enable **Use DHCP** to Obtain an IP address automatically to dynamically configure IPv4 address using DHCP.
2. If the field is disabled, enter the **IPv4 Address**, **Subnet Mask** and **Default Gateway** in the respective fields.
3. If you wish to enable the IPv6 settings, check **Enable**.
4. If the IPv6 setting is enabled, enable or disable the option **Use DHCP** for obtaining the IP address automatically.
5. If the field is disabled, enter the **IPv6 Address**, **Subnet Prefix length** and **Default Gateway** in the given field.
6. Click **Save** to save the entries
7. Click **Reset** if you want to reset the modified changes.
NTP

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 page, click Configuration > NTP from the main menu. A sample screenshot of NTP Settings Page is shown in the screenshot below.

NTP Settings page

The fields of Configuration – NTP are explained below.

**Date:** To specify the current date of the device

**Time:** Specify the current Time for the device.

  **Note:** As Year 2038 Problem exists, Date and Time should be configured within the range.

**NTP Server:** Specify the NTP Server for the device.

**UTC Offset:** List box contains UTC offset values for NTP server, which can be used to display to exact local time.

  **Note:** Use correct UTC offset after adjusting for DST.

**Automatically synchronize:** Check the box, to automatically synchronize Date and Time with the NTP Server.

**Refresh:** To reload the current date and time settings.
**Procedure**

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.

In the **NTP Server field**, specify the NTP server for the device.

**Refresh**: Click this field to reload the date and time settings

**Save**: Click this field to save the entries.

**Reset**: Click this field to reset the entries.
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 page, click **Configurations > PEF** from the main menu. A sample screenshot of PEF Management Settings Page is shown in the screen shot below.

Each tabs are explained below.
**Event Filter Tab**

A PEF implementation is recommended to provide at least 16 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, etc. Remaining entries can be made available for ‘OEM’ or System Management Software configured events. Note that 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 reallocated if necessary.

**PEF Management – Event Filter**

The fields of PEF Management – Event Filter Tab are explained below.

This page contains the list of configured PEF’s.

**PEF ID:** This field displays the ID for the newly configured PEF entry (readonly).

**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.

**Cancel:** To cancel the modification and return to Event filter list.
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** to open the Add event Filter entry Page. A sample screenshot of Add Event Filter Page is in seen the screenshot below.

   ![Add Event Filter Entry Page](image)

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

   **NOTE:** Alert Policy has to be configured - under Configuration->PEF->Alert Policy.

5. In the Generator ID configuration section,
   • 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.

   **NOTE:** In RAW data field, to specify hexadecimal value prefix with '0x'.

6. 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.

   • In the Slave Address/Software ID field, Specify corresponding I2C Slave Address or System Software ID.
   • 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.
   • Choose the corresponding IPMB device LUN if event generated by IPMB.

7. In the Sensor configuration section,
   • Select the s type of sensor that will trigger the event filter action.
   • In the sensor name field, choose the particular sensor from the sensor list.
   • Choose event option to be either All Events or Sensor Specific Events.

8. In the Event Data configuration section,
   • Event Trigger field is used to give Event/Reading type value.

   **NOTE:** Value ranges from 1 to 255.

   • Event Data 1 AND Mask field is used to indicate wildcarded or compared bits.

   **NOTE:** Value ranges from 0 to 255.

   • Event Data 1 Compare 1 & Event Data 1 Compare 2 field is used to indicate whether each bit position's comparison is an exact comparison or not.

   **NOTE:** Value ranges from 0 to 255.

9. In the Event Data 2 configuration section,
• Event Data 2 AND Mask field is similar to Event Data 1 AND Mask.
• Event Data 2 Compare 1 & Event Data 2 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
9. In the Event Data 3 configuration section,
• Event Data 3 AND Mask field is similar to Event Data 1 AND Mask.
• Event Data 3 Compare 1 & Event Data 3 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
10. Click **Modify** to accept the modification and return to Event filter list.
11. Click **Reset** to reset the modification done.
12. Click on **Cancel** to cancel the modification and return to Event filter list.
13. In the Event filter list, click **Modify** to modify the existing filter.
14. In the Event filter list, click **Delete** to delete the existing filter.
**Alert Policy Tab**

This page is used to configure the Alert Policy and LAN destination. You can add, delete or modify an entry in this page.

**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 (readonly).

**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.
- **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.
Cancel: To cancel the modification and return to Alert Policy list.
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, then 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 to open the Add Alert Policy Entry Page as shown in the screenshot below.

3. Policy Entry # is a read only field.

4. Select the Policy Number from the list.

5. In the Policy Configuration field, check Enable if you wish to enable the policy settings.

6. In the Policy Set field, choose any of the Policy set from the list.

7. In the Channel Number field, choose particular channel from the available channel list.

8. 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, then you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destination tab.

9. In the Alert String field, enable the check box if the Alert policy entry is Event Specific.

10. In the Alert String Key field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.

11. Click Add to save the new alert policy and return to Alert Policy list.

12. Click Cancel to cancel the modification and return to Alert Policy list.

13. In the Alert Policy list, to modify a configuration, select the slot to be modified and click Modify.

14. In the Modify Alert Policy Entry Page, make the necessary changes and click Modify.

15. In the Alert Policy list, to delete a configuration, select the slot and click Delete.
**PEF Management LAN Destination Page**

This page is used to configure the Event filter, Alert Policy and LAN destination. A sample screenshot of PEF Management LAN Destination Page is given below.

**PEF Management LAN Destination**

The fields of PEF Management – LAN Destination Tab are explained below.

**LAN Destination:** Displays Destination number for the newly configured entry (readonly).

**Destination Type:** Destination type can be either an SNMP Trap or an Email alert. For Email alerts, the 3 fields - destination Email 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.

**Destination Address:** If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:

- IPv4 address format.
- IPv6 address format.

If Destination type is Email Alert, then give the email address that will receive the email.

**Subject & Message:** These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address in case of any severity events with a subject specified in subject field and will contain the message field’s content as the email body.

**Add:** To save the new LAN destination and return to LAN destination list.

**Cancel:** To cancel the modification and return to LAN destination list.
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, then you have to configure the 4th slot of LAN Destination Page.

2. Select the slot and click **Add**. This opens the **Add LAN Destination entry**.

3. In the **LAN Destination** field, the destination for the newly configured entry is displayed and this is a read only field.

4. In the **Destination Type** field, select the one of the types.

5. In the **Destination Address** field, enter the destination address.

   **NOTE**: If Destination type is Email Alert, then give the email address that will receive the email.

6. Select the **User Name** from the list of users.

7. In the **Subject** field, enter the subject.

8. In the **Message** field, enter the message.

9. Click **Add** to save the new LAN destination and return to LAN destination list.

10. Click **Cancel** to cancel the modification and return to LAN destination list.

11. In the LAN Destination Tab, to modify a configuration, select the row to be modified and click **Modify**.

12. In the **Modify LAN Destination Entry** page, make the necessary changes and click **Modify**.

13. In the LAN Destination Tab, to delete a configuration, select the slot and click **Delete**.
RADIUS

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.

In MegaRAC GUI, this page is used to set the RADIUS Authentication.

To open RADIUS Settings page, click **Configuration > RADIUS** from the main menu. A sample screenshot of RADIUS Settings Page is shown in the screenshot below.

![RADIUS Settings Page](image)

RADIUS Settings Page
The fields of RADIUS Settings Page are explained below.

**RADIUS Authentication:** Option to enable RADIUS authentication.

**Port:** The RADIUS Port number.

  **Note:**
  - Default Port is 1812.

**Time Out:** The Time out value in seconds.

  **Note:**
  - Default Timeout value is 3 seconds.
  - Timeout value ranges from 3 to 300.

**Server Address:** The IP address of RADIUS server.

  **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.

**Secret:** The Authentication Secret for RADIUS server.

  **Note:**
  - This field will not allow more than 31 characters.
  - Secret must be at least 4 characters long.
  - White space is not allowed.

**Save:** To save the settings.

Reset: To reset the modified changes.
**Procedure**

1. Enable the **RADIUS Authentication** checkbox to authenticate the RADIUS.
2. Enter the port number in the **Port Number** field.
3. Enter the time out value in seconds in the **Time out** field.
4. Enter the address of the server in the **Server Address** field.
5. Enter the authentication secret for RADIUS Server in the **Secret** field.
6. Click **Save** to save the entered details.
7. Click **Reset** to reset the entered details.
Remote Session

In MegaRAC SP, use this page to configure virtual media configuration settings for the next redirection session. Encryption is disabled by default.

To open Remote Session page, click Configuration > Remote Session from the main menu. A sample screenshot of Remote Session Page is shown in the screenshot below.

Remote Session

The fields of SMTP Settings Page are explained below.

KVM Encryption: Enable/Disable encryption on KVM data for the next redirection session.

Media Encryption: Enable/Disable encryption on Media data for the next redirection session.

Virtual Media Attach Mode: Two types of VM attach mode are available:

- **Attach** - Immediately attaches Virtual Media to the server upon bootup.
- **Auto Attach** - Attaches Virtual Media to the server only when a virtual media session is started.

Save: To save the current changes.

Note: It will automatically close the existing remote redirection either KVM or Virtual media sessions, if any.

Reset: To reset the modified changes.
Procedure

1. In **KVM encryption**, check or uncheck the option **Enable**.
2. In **Media Encryption**, check or uncheck the option **Enable**.
3. In **Virtual media Attach mode**, select **Auto Attach** or **Attach** from the dropdown list as required.
4. Click **Save** to save the entries.
5. Click **Reset** to reset the entries.

**Note:**

If we choose more than one virtual CDROMs, then the RHEL5 host displays only one CDROM in the “Computer” window. When we redirect second CDROM, the second CDROM device will appear in “Computer” window.

If we choose more than 2 virtual Hard disks, then the RHEL5 host displays only two hard disks in “Computer” window. When we redirect third hard disk, the third hard disk will appear in “Computer” window.
SMTP

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

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

To open SMTP Settings page, click Configuration > SMTP from the main menu. A sample screenshot of SMTP Settings Page is shown in the screenshot below.

SMTP Settings Page

The fields of SMTP Settings Page are explained below.

**Port:** The name of the SMTP Port.

  Note: Default Port is 25.

**SMTP Server IP:** The IP address of the SMTP Server.

  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.
  - IPv6 Address made of 8 numbers separated by colon "::" or double colon ":::". Eg: 2004::2010
  - Each field ranges from 0 to FFFF.

**Sender Address:** The email address of the sender valid on the SMTP Server.

**Machine Name:** Name of the SMTP Server.

  - Machine Name is a string of maximum 15 alpha-numeric characters.
Space and special characters are not allowed.

**SMTP Server requires Authentication:** Option to enable SMTP Authentication.

Note: Server Authentication Types supported are:

- 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:** Username using which you wish to access SMTP Accounts.

Note:

- User Name can be of length 4 to 15 alpha-numeric characters.
- It must start with an alphabet.
- Special characters ',', ':' (colon), ';' (semicolon), ' ' (space) and '\' (backslash) are not allowed.

**Password:** Password for the SMTP User Account.

Note: This field will not allow more than 19 characters.

- Password must be at least 4 characters long.
- White space is not allowed.

**Save:** To save the entries.

**Reset:** To reset the entries.
Procedure

1. Enter the **Port Name** of the SMTP Server in the field given.
2. Enter the **SMTP Server IP** in the field given.
3. Enter your email address in the **Sender Address** field.
4. Enter the IPMI machine name in the **Machine Name** field.
5. Enable the check box **SMTP Server requires Authentication** if you want to authenticate SMTP Server.
6. Enter your **User name** in the given field.
7. Enter your **Password** in the given field.
8. Click **Save** to save the entered details.
9. Click **Reset** to update the entered details.
SNMP

In MegaRAC GUI, this page to configure the SNMP settings. Simple Network Management Protocol (SNMP) is a UDP-based network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

To open SNMP Settings page, click Configuration > SNMP from the main menu. A sample screenshot of SNMP Settings Page is shown in the screenshot below.

> SNMP Settings

The following fields are displayed in this page.

**SNMPv1/v2 Configuration** - To enable or disable SNMPv1 & SNMPv2c features.

**Access Level** - The access level option to communicate with SNMP which could be either Read Only or Read Write.

**Community String** - Community string is match in both SNMPv1 and SNMPv2c.

- A string of 4 to 15 characters.
- It is an optional field

**SNMPv3 Configuration** – To enable or disable the SNMPv3 features.

**User Account** - The user name of the SNMPv3 user.
- User Name can be of length 4 to 15 alpha-numeric characters.
- It must start with an alphabet.
- Special characters ',', ':'(colon), ';'(semicolon), ' '(space) and '\'(backslash) are not allowed.

**User Access** - The Access level option for SNMPv3 user which could be either it can be Read Only or Read Write.


**Authentication Passphrase** - Specify the authentication password for Authentication protocol.
- Password must be at least 8 characters long.
- White space is not allowed.
  
  **Note:** This field will not allow more than 20 characters.

**Privacy protocol** - The Encryption algorithm to use for SNMPv3 settings.

**Privacy Passphrase** - The privacy password for Privacy protocol.
- Password must be at least 8 characters long.
- White space is not allowed.
  
  **Note:** This field will not allow more than 20 characters.

**Save** – To save the SNMP configuration.

**Reset** - To reset the modified changes.

**Procedure**

1. Check the option **Enable** to enable the SNMP v1 and SNMPv2c features.
2. Choose the **Access level** option to communicate with SNMP.
3. If the SNMP v1/v2 Configuration is enabled, select the Access Level.
4. Enter the **Community String**.
5. Enable **SNMPv3 Configuration**.
6. Specify the **User Account**.
7. Select the **User Access** – Read only or Read Write.
8. Choose the **Authentication Protocol** from the dropdown list.
9. Enter the **Authentication Passphrase**.
10. Choose the **Privacy Protocol** from the dropdown list.
11. Enter the **Privacy Passphrase**.
12. Click **Save** to save the entered configuration.
SSL

The **Secure Socket Layer** protocol was created by Netscape to ensure 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, you can upload the new SSL certificate. Using the SSL certificate, the device can be accessed in a secured way. The Current Certificate and policy key will be displayed in this page.

To open SSL Management page, click **Configuration > SSL** from the main menu. A sample screenshot of SSL Management Page is shown in the screenshot below.

![SSL Management Page](image)

SSL Management Page

The fields of SSL Management Page are explained below.

- **Current Certificate**: Displays the date and time on which the certificate is uploaded
- **Current Privacy Key**: Displays the time and date on which the Privacy Key is set.
- **New SSL Certificate**: To select the new SSL certificate to be uploaded.
- **Upload**: To upload the certificate that is browsed.
- **Cancel**: To cancel the upload.
**Procedure**

1. **Browse** and select the certificate to be uploaded.
2. Click **Upload**.
3. Upload the privacy key when a prompt message appears to upload the privacy key.
4. On successful upload, a success message is shown.

**Note:** Both the files should be of the type PEM.

- Once you upload the certificates, click **OK** to reset MegaRAC® SP.

- 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 192.168.0.30, enter the following: https://192.168.0.30

- Please note the `<s>` after `<http>`. You must accept the certificate before you are able to access your Generic MegaRAC® SP.
System and Audit Log

In MegaRAC GUI, System and Audit log page displays a list of system logs and audit logs occurred in this device.

To open System and Audit log page, click **Configuration > System and Audit Log** from the main menu. A sample screenshot of System and Audit Log Settings Page is shown in the screenshot below.

![System and Audit Log Settings](image)

**System and Audit Log settings**

The fields of System and Audit Log Settings Page are explained below.

**System Log:** This field is to enable or disable the system logs.

**Log Type:** Specifies the Log type for system logs, whether it should be preserved in a local file or on a remote server.

- **File Size:** This field is 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, then old log information gets cleared permanently.

**Server Address:** This field is to specify the remote server address to the log 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

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 is 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. In the Server Address field, enter the server address.
5. In the Audit Log field, check or uncheck the Enable option as desired.
6. Click Save to save the changes.
7. Click Reset to reset the entries.
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.

To open User Management page, click **Configuration > Users** from the main menu. A sample screenshot of User Management Page is shown in the screenshot below.

![User Management Page](image)

**User Management Page**

The fields of User Management Page are explained below.

**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.

**Email ID:** Displays email address of the user.

**Network Privilege:** Displays the network access privilege 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

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

Add a new user:

1. To add a new user, select a free slot and click Add User. This opens the Add User screen as shown in the screenshot below.

![Add User Page]

2. Enter the name of the user in the User Name 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 ',', '.', '(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.

4. Note:
   - Password must be at least 8 characters long.
   - White space is not allowed.
   - This field will not allow more than 20 characters.

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.

7. In the New SSK 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.

**Modify an existing User**

10. Select an existing user from the list and click **Modify User**. This opens the Add User screen as shown in the screenshot below.

![Modify User Page](image)

11. Edit the required fields.
12. To change the password, enable the **Change Password** option.
13. After editing the changes, click Modify to return to the users list page.

**Delete an existing User**

14. To delete an existing user, select the user from the list and click **Delete User**.
Virtual Media

In MegaRAC GUI, this page to configure Virtual Media device settings. If you change the configuration of the virtual media in this page, it shows the appropriate device in the JViewer Vmedia dialog. For example, if you select two floppy devices in Configure Virtual Media page, then in JViewer Vmedia, you can view two floppy device panel.

To open Virtual Media page, click **Configuration > Virtual Media** from the main menu. A sample screenshot of User Management Page is shown in the screenshot below.

Configure Virtual Media Devices

The following fields are displayed in this page.

**Floppy devices:** The number of floppy devices that support for Virtual Media redirection.

**CD/DVD devices:** The number of CD/DVD devices that support for Virtual Media redirection.

**Harddisk devices:** The number of harddisk devices that support for Virtual Media redirection.

**Local Media Support:** To enable or disable the local media support for Virtual Media redirection.

**Save:** To save the configured settings.

**Reset:** To reset the previously-saved values.
**Procedure**

1. Select the number of Floppy devices, CD/DVD devices and Harddisk devices from the dropdown list
   
   **Note:** Maximum of two devices can be added in Floppy, CD/DVD and Harddisk drives.

2. Enable the **Local Media Support** if needed.

3. Click **Save** to save the changes made else 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.

For more details refer [VMedia](#)
Remote Control

The Remote Control consists of the following.

- Console Redirection
- Server Power Control

A sample screenshot of the Remote Control menu is given below.

![Remote Control Menu](image)

Remote Control Menu

A detailed description of the menu items are given ahead.
Console Redirection

The remote console application, which is started using the WebGUI, allows you to control your server’s operating system 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.

Browser Settings

For Launching the KVM, pop-up block should be disabled. For Internet explorer, enable the download file options from the settings.

Java Console:

This is an OS independent plug-in which can be used in Windows as well as Linux with the help of JRE. JRE should be installed in the client’s system. You can install JRE from the following link:

**Procedure**

In MegaRAC GUI, the Java Console can be launched in two ways

1. Open the Dashboard Page and in Remote control section, click Launch for Java Console.
2. Open **Remote Control>Console Redirection** Page and click **Java Console**.

This will download the `.jnlp` file from BMC.

To open the `.jnlp` file, use the appropriate JRE version (Javaws)

When the downloading is done, it opens the Console Redirection window.
Console Redirection Menu

The Console Redirection main menu consists of the following menu items.

- Video
- Keyboard
- Mouse
- Options
- Media
- Keyboard Layout
- Help

A detailed explanation of these menu items are given below.

Video

This menu contains the following sub menu items.

**Pause redirection:** This option is used for pausing Console Redirection.

**Resume Redirection:** This option is used to resume the Console Redirection when the session is paused.

**Refresh Video:** This option can be used to update the display shown in the Console Redirection window.

**Turn Off Host display:** 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.

**Full Screen:** This option is used 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:** This option is used to exit the console redirection screen
Keyboard

This menu contains the following sub menu items.

Hold Right Ctrl Key: This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.

**Hold Right Alt Key:** This menu item can be used to act as the right-side <ALT> key when in Console Redirection.

**Hold Left Ctrl Key:** This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.

**Hold Left Alt Key:** This menu item can be used to act as the left-side <ALT> key when in Console Redirection.

**Left Windows Key:** This menu item can be used to act 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:** This menu item can be used to act 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.

**Alt+Ctrl+Del:** This menu item can be used to act as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the server that you are redirecting.

**Context menu:** This menu item can be used to act as the context menu key, when in Console Redirection.
**Mouse**

**Show Cursor:** This menu item can be used to show or hide the local mouse cursor on the remote client system.

**Mouse Calibration:** This menu item can be 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. Please use '+' or '-' keys to change the threshold settings until both the cursors go out of synch. Please detect the first reading on which cursors go out of synch. Once this is detected, use 'ALT-T' to save the threshold value.
Options

**Band width:** The *Bandwidth Usage* option allows you to adjust the bandwidth. You can select one of the following:

- **Auto Detect** - This option is used to detect client system keyboard layout automatically and send the key event to the host based on the Layout detected.
- 256 Kbps
- 512 Kbps
- 1 Mbps
- 10 Mbps

**Keyboard/Mouse Encryption:** This option 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%
Media

Virtual Media Wizard:

To add or modify a media, select and click 'Virtual Media Wizard' button, which pops out a box named "Virtual Media" where you can configure the media. A sample screenshot of Virtual media screen is given below.
**Floppy Key Media:** This menu item can be used to start or stop 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® SPs.

**CD/DVD Media:** This menu item can be used to start or stop the redirection of a physical DVD/CD-ROM drive and cd image types such as iso.

**Hard disc/USB Key Media:** This menu item can be used to start or stop the redirection of a Hard Disk/USB key image, instead of a physical drive and harddisk image.

*Note:*

For windows client, if the logical drive of the physical drive is dismount then the logical device is redirected with Read/Write Permission else it is redirected with Read permission only.

For MAC client, External USB Hard disk redirection is only supported.

For Linux client, fixed hard drive is redirected only as Read Mode. It is not Write mode supported.
Keyboard Layout

**Auto Detect:** This option is used to detect keyboard layout automatically. The languages supported automatically are English – US, French – France, Spanish – Spain, German- Germany, Japanese- Japan. 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.

**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 softkeyboard to avoid typo errors.

   Note: Soft keyboard is applicable only for JViewer Application not for other application in the client system.
**Video Record**

Note: This option is available only when you launch the Java Console.

Important: To view this menu option you must download the Java Media FrameWork (JMF). It can be downloaded from the link [http://www.oracle.com/technetwork/java/javase/download-142937.html](http://www.oracle.com/technetwork/java/javase/download-142937.html)

**Start Record**: This option is to start recording the screen.

**Stop Record**: This option is used to stop the recording.

**Settings**: To set the settings for video recording.

**Procedure**

**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.

![Video Record Settings Page](link)

2. Set the **Frame Interval**.
3. Note: The frame interval value ranges from 0 ms to 2000ms
4. Enter the **Number of Frames** in the given field.
5. **Browse** and enter the location where you want the video to be saved.
6. Select the video type by enabling the check box – **avi**, **mp4**, **mov**, **wmv**.
7. Click **OK** to save the entries and return to the Console Redirection screen.
8. Click **Cancel** if you don’t wish to save the entries.
9. In the Console Redirection window, click **Video Record > Start Record**.
10. Record the process.

11. To stop the recording, click Video Record > Stop Record.

**Help**

*Jviewer:* Displays the copyright and version information
# Quick Buttons

The lower right of Console Redirection windows 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>
<thead>
<tr>
<th>Quick Buttons</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Play Button" /></td>
<td>This key is used to play the Console redirection after being paused.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Pause Button" /></td>
<td>This key can be used for pausing Console Redirection.</td>
</tr>
</tbody>
</table>
| ![Full Screen Button](image3.png) | This button is used to view the Console Redirection in full screen mode.  
Note: Set your client system resolution to 1024x768 so that you can view the server in full screen. |
| ![Soft Keyboard Button](image4.png) | This quick button is used to show or hide the soft keyboard. |
| ![Zoom Button](image5.png) | Drag this to zoom in or out. |
| ![LED Status](image6.png) | These buttons displays the host LED status. |
| ![Record Video Button](image7.png) | This quick button is used to record the video. |
| ![Virtual Media Buttons](image8.png) | These three quick buttons will pop up a virtual media where you can configure the media. |
| ![Mouse Cursor Button](image9.png) | This quick button is used to show or hide the mouse cursor on the remote client system. |
Server Power Control

This page allows you to view and control the power of your server.

To open Power Control and Status page, click **Remote Control > Server Power Control** from the main menu. A sample screenshot of Power Control and Status page is shown in the screenshot below.

![Power Control and Status Page](image)

The various options of Power Control are given below.

**Reset Server**: This option will reboot the system without powering off (warm boot).

**Power Off Server – Immediate**: This option will immediately power off the server.

**Power Off Server – Orderly Shutdown**: This option will initiate operating system shutdown prior to the shutdown.

**Power On Server**: This option will power on the server.

**Power Cycle Server**: This option will first power off, and then reboot the system (cold boot).

**Perform Action**: Click this option to perform the selected operation.

**Procedure**

Select an action and click **Perform Action** to proceed with the selected action.

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

This group of pages allows you to do maintenance tasks on the device. The menu contains two items

- Firmware Update
- Restore Factory Defaults

A detailed description is given ahead.

Firmware Update

In MegaRAC GUI, this wizard takes you through the process of firmware upgradation. A reset of the box will automatically follow if the upgrade is completed or cancelled. An option to preserve configuration will be presented. Enable it, if you wish to preserve configured settings through the upgrade.

**WARNING:** Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will be reset.

**Note:**

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.

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

To open Firmware Update page, click **Maintenance > Firmware Update** from the main menu. A sample screenshot of Firmware Update Page is shown in the screenshot below.

![Firmware Update Page](image-url)
**Procedure**

Click **Enter Update Mode** to upgrade the current device firmware.

**Note:**
You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware. The device will reset if update is canceled. The device will also reset upon successful completion of firmware update.

**Restore Factory Defaults**

In MegaRAC GUI, this option is used to restore the factory defaults of the device firmware.

**WARNING:** Please note that 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.

To open Restore Factory Defaults page, click **Maintenance > Restore Factory Defaults** from the main menu. A sample screenshot of Restore Factory Defaults Page is shown in the screenshot below.

![Restore Factory Defaults Page](image)

**Procedure**

Click **Restore Factory** to restore the factory defaults of the device firmware.
Log Out

To log out of the MegaRAC GUI, click the logout link on the top right corner of the screen.
FLASH Tools

The Flash Tools are command line utility programs used to upgrade the firmware using different medium like KCS, USB, and LAN. There are two tools which are being used.

- YAFUFlash
- YAFUKCS

YAFUFlash:

Yet Another Firmware Upgrade Flash is a tool used for flashing the BMC. This utility is used for flashing in both Linux and Windows environment. There are two types of medium used to flash the BMC. They are,

- Network
- USB

Both mediums are applicable for Windows and Linux environment. The medium can be selected as per your requirement.

Installation in Windows:

1. Open the command prompt an enter YafuFlash\Windows path.
2. This contains two files, Yafuflash.exe and LIBIPMI.dll.
3. Run the Yafuflash.exe in the command prompt
4. Format: Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE], where

   [OPTIONS]
   - info Displays information about existing FW and new FW
   - force-boot Option to FORCE BootLoader upgrade during full upgrade
   - preserve-config Option Preserve configuration module during full upgrade

   [MEDIUM]
   -cd Option to use USB medium
   -nw & -ip Option to network medium with -ip followed by IP address.

   [FW_IMAGE_FILE]
   Firmware image file name [rom.ima].
Examples for Network Medium

**Eg1:** Yafuflash –nw –ip 155.166.132.12 –info rom.ima

**Description:** This command works with network medium using the ip 155.166.132.12, which displays the details of both Existing Firmware and new firmware.

**Eg2:** Yafuflash –nw –ip 155.166.132.12 rom.ima

**Description:** This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware.

**Eg3:** Yafuflash –nw –ip 155.166.132.12 –force-boot rom.ima

**Description:** This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware with FORCE BootLoader Upgrade.

**Eg4:** Yafuflash –nw –ip 155.166.132.12 –preserve-config rom.ima

**Description:** This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware with preserve config params.

**Eg5:** Yafuflash –nw –ip 155.166.132.12 –force-boot –preserve-config rom.ima

**Description:** This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware with FORCE BootLoader Upgrade and preserve config params.

Examples for USB Medium:

**Eg1:** Yafuflash –cd –info rom.ima

**Description:** This command works with USB medium which displays the details of both Existing Firmware and new firmware.

**Eg2:** Yafuflash –cd rom.ima

**Description:** This command works with USB medium which start to flash the new rom.ima to the firmware.

**Eg3:** Yafuflash –cd –force-boot rom.ima

**Description:** This command works with USB medium which start to flash the new rom.ima to the firmware with FORCE BootLoader Upgrade.

**Eg4:** Yafuflash –cd –preserve-config rom.ima

**Description:** This command works with USB medium which start to flash the new rom.ima to the firmware with preserving config params.

**Eg5:** Yafuflash –cd –force-boot –preserve-config rom.ima
Description: This command works with USB medium which start to flash the new rom.ima to the firmware with FORCE BootLoader Upgrade and preserving config params.

Installation in Linux

1. Open Terminal and go to YafuFlash/Linux path.
2. Run the Yafuflash.exe in the terminal
3. Format: ./Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE] where,

   [OPTIONS]
   - info Displays information about existing FW and new FW
   - force-boot Option to FORCE BootLoader upgrade during full upgrade
   - preserve-config Option Preserve configuration module during full upgrade

   [MEDIUM]
   -cd Option to use USB medium
   - nw & -ip Option to network medium with –ip followed by IP address.

   [FW_IMAGE_FILE]
   Firmware image file name [rom.ima].

Examples of Network Medium:

Eg1: ./Yafuflash –nw –ip 155.166.132.12 –info rom.ima
Description: This command works with network medium using the ip 155.166.132.12, which displays the details of both Existing Firmware and new firmware.

Eg2: ./Yafuflash –nw –ip 155.166.132.12 rom.ima
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware.

Eg3: ./Yafuflash –nw –ip 155.166.132.12 –force-boot rom.ima
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware with FORCE BootLoader upgrade.

Eg4: ./Yafuflash –nw –ip 155.166.132.12 –preserve-config rom.ima
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware with preserving config params.
Eg5:  

./Yafuflash –nw –ip 155.166.132.12 –force-boot –preserve-config rom.ima

**Description:** This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware with FORCE BootLoader upgrade and preserving config params.

![Screen: If Existing and current images are same.](image)
YAFUKCS:

Yet Another Firmware Upgrade Keyboard Controller Style is a tool used for flashing the firmware. This Utility is used for flashing in DOS environment and is used particularly in the Keyboard Controller Style (KCS) interface.

Installation:

1. Copy Yafukcs.exe into DOS machine
2. Run Yafukcs utility.
3. Format: Yafukcs [OPTION] [FW_IMAGE_FILE], where
   -info Displays information about existing firmware and new firmware
   -force-boot Option to FORCE BootLoader upgrade during full upgrade
   -preserve-config Option Preserve configuration module during full upgrade
   [FW_IMAGE_FILE]
   - Firmware image file name [rom.ima].

Examples:

Eg1: ./Yafukcs –info rom.ima
Description: Displays the details of both Existing Firmware and new firmware.

Eg2: ./Yafukcs rom.ima
Description: This command starts to flash the new rom.ima to the firmware.

Eg3: ./Yafukcs –force-boot rom.ima
Description: This command starts to flash the new rom.ima to the firmware with FORCE BootLoader upgrade.

Eg4: ./Yafukcs –preserve-config rom.ima
Description: This command starts to flash the new rom.ima to the firmware with preserving config params.

Eg5: ./Yafukcs –force-boot –preserve-config rom.ima
**Description**: This command starts to flash the new rom ima to the firmware with FORCE BootLoader upgrade and preserving config params.
VMCLI Tool

VMCLI (Virtual Media Command line interface):

The Virtual Media Command Line Interface (VMCLI) utility is a scriptable command-line interface that provides virtual media features from the management station to the Host.

VMCLI is used to redirect the virtual media (Hard Disk, Floppy, CD drive, USB..) from the management station to the host.

Features:

- Removable media devices or image files that are consistent with the Virtual Media plug-ins
- Automatic termination when the host firmware boot once option is enabled
- Secure communication to the host using Secure Sockets Layer (SSL)

Installation in Windows

1. Open Command Prompt and go to VMCLI folder.
   Note: You must keep wget inside the VMCLI Folder, which is the support Tool for VMCLI
2. Run the VMCLI.exe in the command prompt
3. Format:
   VMCLI.exe [-r] [IP : PORT] [-u][RAC-USER] [-p] [RAC- PASSWORD] [MEDIA TYPE] [MEDIA][-e], where
   [IP: PORT] IP Address: Port Number
   IPv4 IPv4 format address
   IPv6 Not supported
   Note: Port number is optional
   [RAC- USER] User Name
   User id, with 'virtual media' privilege
[RAC- PASSWORD] Password

User password, with 'virtual media' privilege

[MEDIA TYPE]

-c CD/DVD Drive and CD/DVD Image
-f Floppy Drive and Floppy Image
-hd Hard Disk Drive, Hard Disk Image and USB

[MEDIA]

Media drive (or) Media Image

Media Drive For Hard Disk Drive need to mention only physical drive volume like physicaldrive0, physicaldrive1 etc

To know physical drive volumes go to Control panel -> Administrative Tools-> Computer Management -> Storage-> Disk Management (Refer Image 1.0)

-[E] Enable encrypted data transfer through ssl
Examples of Floppy Media redirection

Eg1:     VMCLI.exe -r 10.0.6.8:443 -u root -p superuser -f A: /
Description: This command is to redirect the floppy disk media from the management station to the host.

Eg2:     VMCLI.exe -r 10.0.6.8 -u root -p superuser -f FloppyImage.img
Description: This command is to redirect the floppy disk image from the management station to the host.

Eg3:     VMCLI.exe -r 10.0.6.8 -u root -p superuser -f FloppyImage.img -e
Description: This command is to redirect the floppy image media from the management station to the host. Data will be transferred through ssl.

Examples of CD-ROM Media redirection

Eg1:     VMCLI.exe -r 10.0.6.8 -u root -p superuser -c E: /
Description: This command is to redirect the CD/DVD media from the management station to the host.

Eg2:     VMCLI.exe -r 10.0.6.8:443 -u root -p superuser -c E: / -e
Description: This command is to redirect the CD/DVD media from the management station to the host. Data will be transferred through ssl.

Eg3:     VMCLI.exe -r 10.0.6.8 -u root -p superuser -c CD-RomImage.iso
Description: This command is to redirect the CD/DVD image from the management station to the host.
Examples of Hard Disk Drive Media redirection

Eg1: \texttt{VMCLI.exe -r 10.0.6.8 -u root -p superuser -hd physicaldrive0}

\textbf{Description:} This command is to redirect the Hard disk media from the management station to the host.

Eg2: \texttt{VMCLI.exe -r 10.0.6.8 -u root -p superuser -hd physicaldrive0 -e}

\textbf{Description:} This command is to redirect the Hard disk media from the management station to the host. Data will be transfer through ssl.

Eg3: \texttt{VMCLI.exe -r 10.0.6.8 -u root -p superuser -hd HardDiskImage.img}

\textbf{Description:} This command is to redirect the Hard disk image from the management station to the host.
Installation in Linux

1. Open Terminal and go to VMCLI folder
2. Run the VMCLI in the Terminal
3. Format:
   ```
   VMCLI.exe [-r] [IP:PORT] [-u] [RAC-USER] [-p][ RAC-PASSWORD] [MEDIA TYPE] [MEDIA] [-e], where
   
   [IP:PORT]       IP Address:Port Number
   IPv4            IPv4 format address  E.g.: 10.0.6.8:443
   IPv6            IPv6 format address  E.g.: [2004::2000]:443
   
   IP should be given with in Ankle bracket like [2004::2000] for IPV6
   
   Note: Port number is optional
   
   [RAC-USER]       User Name
   
   User id, with 'virtual media' privilege
   
   [RAC-PASSWORD]   Password
   
   User password, with 'virtual media' privilege
   
   [MEDIA TYPE]
   
   -c              CD/DVD Drive and CD/DVD Image
   ```
Examples of Floppy Media redirection

**Eg1:**
IPv4: ./VMCLI -r 10.0.6.8 -u root -p superuser -f /dev/sdb  

**Description:** This command is to redirect the floppy disk media from the management station to the host.

**Eg2:**
IPv4: ./VMCLI -r 10.0.6.8:443 -u root -p superuser -f /dev/sdb -e  

**Description:** This command is to redirect the floppy image media from the management station to the host. Data will be transfer through ssl.

**Eg3:**
IPv4: ./VMCLI -r 10.0.6.8:443 -u root -p superuser -f FloppyImage.img  

**Description:** This command is to redirect the floppy image media from the management station to the host.

**CD-ROM Media redirection**

**Eg1:**
IPv4: ./VMCLI -r 10.0.6.8 -u root -p superuser -c /dev/sdc  

**Description:** This command is to redirect the CD/DVD media from the management station to the host.

**Eg2:**
IPv4: ./VMCLI -r 10.0.6.8:443 -u root -p superuser -c CD-RomImage.iso  

**Description:** This command is to redirect the CD/DVD image from the management station to the host.

**Eg3:**
IPv4: ./VMCLI -r 10.0.6.8 -u root -p superuser -c CD-RomImage.iso -e

Description: This command is to redirect the CD/DVD media from the management station to the host. Data will be transfer through ssl.

Hard Disk Drive Media redirection

Eg1:  IPv4 :./VMCLI -r 10.0.6.8 -u root -p superuser -hd /dev/sda
IPv6 :./VMCLI -r [2004::2000]:443 -u root -p superuser -hd /dev/sda

Description: This command is to redirect the Hard disk from the management station to the host.

Eg2:  IPv4 :./VMCLI -r 10.0.6.8 -u root -p superuser -hd HDDImage.img

Description: This command is to redirect the Hard disk image from the management station to the host.

Eg3:  IPv4 :./VMCLI -r 10.0.6.8:443 -u root -p superuser -hd /dev/sda -e

Description: This command is to redirect the Hard disk from the management station to the host. Data will be transfer through ssl.
FG: 2 Existing and current are different.

**Examples for USB Medium:**

**Eg1:**  
```
/Yafuflash –cd –info rom.ima
```

**Description:** This command works with USB medium which displays the details of both Existing Firmware and new firmware.

**Eg2:**  
```
/Yafuflash –cd rom.ima
```

**Description:** This command works with USB medium which start to flash the new rom.ima to the firmware.

**Eg3:**  
```
/Yafuflash –cd –force-boot rom.ima
```

**Description:** This command works with USB medium which start to flash the new rom.ima to the firmware with FORCE BootLoader upgrade.

**Eg4:**  
```
/Yafuflash –cd –preserve-config rom.ima
```

**Description:** This command works with USB medium which start to flash the new rom.ima to the firmware with preserving config params.
Eg5: ./Yafuflash –cd –force-boot –preserve-config rom.ima

**Description:** This command works with USB medium which start to flash the new rom.ima to the firmware with FORCE BootLoader upgrade and preserving config params.
Overview

SMASH-CLP (System Management Architecture for Server Hardware – Command Line Protocol) simplifies Cross-Platform management, and provides a simple and generic way to expose and manage the manageable entities via CIM broker.

The SM CLP is a command/response protocol, transmitted and received over a text message-based transport protocol. The SM CLP input syntax defines a set of text-based commands, which include standard verbs and options that operate on command targets and properties described by the CIM schema. Here, each manageable element i.e. CIM Object is termed as ‘targets’, each CIM class is represented as UFCT (User friendly class tag), CIM instances as UFIT (user friendly instance tag). There are 13 set of standard verbs & 12 options defined in SMASH-CLP to manage the server. Thereby, SM CLP enables data center administrators to securely manage their heterogeneous server environments using a command line protocol and a common set of commands.

DMTF characterizes it as CIM having a lexicon of nouns, which SMASH harnesses to reduce its commands down to a couple of verbs. As well as managing servers as a whole, SMASH addresses individual components. A server, for example, may have multiple processors, sensors, network cards, logical devices and cooling systems. SMASH CLP can be directed at specific processors, components and subcomponents. Therefore, one can set up a script to periodically check the temperature sensors on all machines so one can see how the power and AC needs can be adjusted during the day or night to avoid overheating of equipment, or reduce the electric bill safely.

Smashclp is developed in reference & compliance to the following DMTF documents.

- SMASH Implementation Requirements ( DSP 0217)
- SM CLP Spec. ( DSP 0214)
- SM ME Addressing Spec. ( DSP 0215)
- SM CLP to CIM Common Mapping spec ( DSP0216)
- CIM Profiles (DSP 01xxx)
- SM CLP mapping to every CIM Profile ( DSP 08xxx)
Starting SMASHCLP

Steps to be followed to start smashclp

1. Login to the BMC

2. Open /etc/passwd file and edit the first line.
   Change
   
   root:x:0:0:root:/root/usr/local/bin/defshell
   
   to
   
   root:x:0:0:/bin/sh

3. SMASH CLP shall be established through Secure Shell (SSH) as specified below.
   - To connect from a Linux machine, use ‘ssh <BMC ip address>’. Then enter the password
   - To connect from other machines, use a terminal emulator application like putty. In the
terminal emulator application, enter the BMC ip address and choose the connection type as
‘SSH’. Then enter the password when prompted.

4. After successful SSH session, start SMASH CLP by issuing the following commands.
   - smashclpd
   This command discovers the targets (Manageable Elements). After successful discovery
   following message will be displayed
     
     SMASHCLPD Connection Established & Started...!
   
   - smashclp
   
   This command starts SMASH CLP as specified below.
     
     >> SMASH-CLP <<
     
     →
**Standard CLP Verbs**

**cd Verb:**

This verb is used to navigate to the particular target address space in the MAP (Manageability Access Point).

Eg: The below command 'cd /admin1' will navigate to the admin target.

```
$ cd /admin1
COMMAND OK :

ufip=/admin1
```

**show verb**

This verb is used to show the information about a particular target/collection or association. It displays the sub-targets contained within the given target, its properties, supported operation (verbs) & list of other targets to which it is associated.

Eg: The below command 'show /admin1/system1/sp1/sshsvc1' will display all the information about SSH Service.

```
$ show /admin1/system1/sp1/sshsvc1
COMMAND OK :

ufip=/admin1/system1/sp1/sshsvc1

Targets:

    profile1/
    sshsetting1/

Associations:
```
ElementConformsToProfile=>/admin1/system1/sp1/sshsvc1/profile1
ElementSettingData=>/admin1/system1/sp1/sshsvc1/sshsetting1
HostedService=>/admin1/system1/sp1

Properties:

SystemCreationClassName=DCIM_ComputerSystem
CreationClassName=DCIM_ProtocolService
SystemName=IPMI Controller 32
Name=SSHProtocolService
Protocol=2
MaxConnections=0
RequestedState=2
EnabledState=2
ElementName=SSH Service
HealthState=7

Verbs:

show
help
cd
version

**exit Verb**

This verb is used to exit from the SMASHCLP session.

Eg: The below command ‘exit’ will terminate the SM CLP appln.

-> exit

COMMAND OK :
exit
**help verb**

This verb is used to get context sensitive help. The functionality is the same as the – help option with the addition of help for targets.

**Eg:** The below command ‘help’ will display the usage of SM CLP.

```plaintext
-> help
COMMAND OK :
help

Welcome to AMI SMASH CLP Implementation!!!

SMASH CLP is a command line interface for the remote user to the server. The commands are of the form of `<verb><options><targets><target-properties>`.

Commands List: cd
    Create
    Delete
    Dump
    Exit
    Help
    Load
    Reset
    Set
    Show
    Start
    Stop
**Version**

Targets: SMASH provides supports targets for SDR, SEL and FRU. The target list for SMASH will depend upon the fore-mentioned files. The most common targets are system1, sensor, tempsensor, etc.

For a comprehensive help please refer to the HELP Manual!!

**version verb**

This verb is used to query the version of the CLP implementation (by default) and other CLP elements (when specified).

Eg: The below command ‘version’ will display the SM CLP version.

-> version

COMMAND OK :
version

*******************************************************************************

CLP Version :1.0.2
SM ME Addressing Version :1.0.0

*******************************************************************************

**set verb**

This verb is used to modify a property or set of properties of a target to a specific value.

Eg: The below command 'set /admin1/system1/sp1 ElementName=ibmc' will change the ElementName property value of sp1 target.

-> set /admin1/system1/sp1 ElementName=ibmc

COMMAND OK :
set /admin1/system1/sp1 ElementName=ibmc
ufip=/admin1/system1/sp1

Properties:
    Name=IPMI Controller 32
    CreationClassName=DCIM_ComputerSystem
    ElementName=ibmc
    EnabledState=2
    RequestedState=11
    HealthState=5
    IdentifyingDescriptions={Manufacturer ID-Product ID}
    OtherIdentifyingInfo={16220-187170}
    OperationalStatus={2}
    Dedicated={28}

**start verb**

This verb is used to cause a target with power/process control to change states to a higher run level.

Eg: The below command `start /admin1/system1` will power on the host system.

    -> start /admin1/system1
    COMMAND OK :
    start /admin1/system1
    ufip=/admin1/system1

    START successful for /admin1/system1

**stop verb**

This verb is used to cause a target with power/process control to change states to a lower run level.

Eg: The below command `stop /admin1/system1` will shutdown the host system.

    -> stop /admin1/system1
COMMAND OK :
stop /admin1/system1

ufip=/admin1/system1
STOP successful for /admin1/system1

reset verb
This verb is used to cause a target with power/process control to cycle states from enabled to disabled and back to enable.

Eg: The below command ‘reset /admin1/system1’ will restart the host system.

-> reset /admin1/system1
COMMAND OK :
reset /admin1/system1

ufip=/admin1/system1
RESET successful for /admin1/system1

delete verb
This verb is used to destroy instances in the address space of the MAP. This is only allowed for specific target object types as defined by the profiles and specific MAP implementation.

Eg: The below command ‘delete /admin1/system1/sp1/account1’ delete the existing account.

-> delete /admin1/system1/sp1/account1
COMMAND OK :
delete /admin1/system1/sp1/account1

ufip=/admin1/system1/sp1/account1

load verb
This verb is used to move a binary image to the MAP from a URI. Its behavior varies for different targets & is detailed in their corresponding DSP 08xxx spec.

-> load -source ftp://myserver.com/pub/fwimage.img
COMMAND OK :
load -source ftp://myserver.com/pub/fwimage.img

LOAD verb is not supported for /

dump verb
This verb is used to move a binary image from the MAP to a URI. Its behavior also varies for different targets & similar to load verb is detailed in their corresponding DSP 08xxx spec.

-> dump -destination ftp://myserver.com/pub/fwimage.img
COMMAND OK :
dump -destination ftp://myserver.com/pub/fwimage.img

DUMP verb is not supported for /

create verb
This verb is used to create new instances and associations in the address space of the MAP. This is only allowed for specific target object types as defined by the profiles and specific MAP implementation.

Eg: The below command 'create /admin1/system1/sp1/account1' tries to create a new account.

-> create /admin1/system1/sp1/account1
COMMAND OK :
create /admin1/system1/sp1/account1

CREATE Verb is not IMPLEMENTED
Standard CLP Verb Options

Output option

This option is used to view the command results in different format. It has many arguments like order, count etc., one of which is ‘format’ which outputs the result in text or clpxml or keyword. By default the output is displayed in text format.

Eg: The below command “cd -o format=clpxml /admin1/system1 “ instructs the command executer to display the output in xml format.

-> cd -o format=clpxml /admin1/system1

COMMAND OK :
cd -o format=clpxml /admin1/system1

<?xml version="1.0" encoding="UTF-8"?>
<response
xmlns="http://schemas.dmtf.org/smash/commandresponse/1.0.0/dsp0224.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="../smash.xsd">
  <command>
    <inputline>cd -o format=clpxml /admin1/system1</inputline>
  </command>
  <cmdstat>
    <status>0</status>
    <status_tag>COMMAND COMPLETED</status_tag>
    <job>
      <job_id>clpjob-36256-4</job_id>
    </job>
  </cmdstat>
</response>
Examine option

Examine option instructs the command processor to check only for the command's validity and correctness but not to execute the command.

Eg: The below command “cd -x /admin1” instructs the command processor to check for the command “cd /admin1”

-> cd -x /admin1

COMMAND OK :
cd -x /admin1

PARSE OK

Display option

Display option is used to filter the information displayed to the user & can be used only with show verb. It has arguments like all, properties, targets, associations & verbs.

Eg 1: The below command “show -d properties /admin1” instructs the command processor to display only the properties of admin target.

-> show -d properties /admin1

COMMAND OK :
show -d properties /admin1

ufip=/admin1

Properties:

    Name=MAP
    CreationClassName=DCIM_AdminDomain
    ElementName=SM CLP Admin Domain

Eg 2: The below command “show -d properties, verbs /admin1” instructs the command processor to display only the properties & verbs of admin target.
-> show -d properties,verbs /admin1
COMMAND OK :
show -d properties,verbs /admin1

ufip=/admin1

Properties:
    Name=MAP
    CreationClassName=DCIM_AdminDomain
    ElementName=SM CLP Admin Domain

Verbs:
    show
    exit
    version
    cd
    help

Help option
Help options instruct the command processor to return the usage of the verb with which this help option is included i.e. show -help will display the decryption & usage of show verb.
Eg: The below command 'exit -help' will display the usage of exit verb.

-> exit -help
COMMAND OK :
exit -help

Command Name: Exit
Used to terminate a CLP session
Usage: exit [-options]

Options: examine – used to examine the command (bypasses executer)

help – shows help on how to use Exit

keep – not implemented

output – Is there to format the output string (should be used with format(clpcsv,keyword,clpxml)

version – shows the smash version

We have few more options like all, source, destination, version, keep, wait, force & level. Refer SM CLP spec DSP0214 to for a detailed description.
The **Common Information Model (CIM)** is an open standard that defines how managed elements in an IT environment are represented as a common set of objects and relationships between them. This is intended to allow consistent management of these managed elements, independent of their manufacturer or provider.

CIM can be accessed using the below mentioned protocols:

- **CIM XML interface** - CIM-XML is a WBEM protocol that uses XML over HTTP to exchange Common Information Model (CIM) information. It uses xml as the payload and HTTP as the transport. It defines all interactions between CIM products as CIM messages.
- **SOAP XML interface** - SOAP stands for Simple Object Access Protocol. It is a communication protocol used for communication between applications via web. It uses both HTTP and HTTPS for transport.

### Profiles supported

Following list of profile supported in SP-X CIM firmware:

- DSP 1007 (SM CLP Admin Domain Profile)
- DSP 1006 (SMASH Collections Profile)
- DSP 1012 (Boot Control Profile)
- DSP 1005 (CLP Service Profile)
- DSP 1018 (Service Processor Profile)
- DSP 1004 (Base Server Profile)
- DSP 1037 (DHCP Client Profile)
- DSP 1038 (DNS Client Profile)
- DSP 1014 (Ethernet Port Profile)
- DSP 1013 (Fan Profile)
- DSP 1036 (IP Interface Profile)
- DSP 1009 (Sensor Profile)
- DSP 1011 (Physical Asset Profile)
- DSP 1027 (Power State Management Profile)
- DSP 1015 (Power Supply Profile)
- DSP 1010 (Record Log Profile)
DSP 1033 (Profile Registration Profile)
DSP 1034 (Simple Identity Management Profile)
DSP 1039 (Role Based Authorization profile)
DSP 1023 (Software Inventory Profile)
DSP 1025 (Software Update Profile)
DSP 1017 (SSH Service Profile)
DSP 1024 (Text Console Redirection)

**CIM Management Instrumentation**

In a CIM enabled environment, model and the upper parts of the CIM infrastructure can be as platform independent as possible. The CIM Management Instrumentation (Provider) is the glue between the model and the managed system and maps the platform independent model to the platform specific resources.

When designing the management instrumentation for a certain platform independent model, it is not satisfying to abstract the provider implementation only upwards to the CIMOM by using CMPI. It is also necessary to layer the implementation of the provider itself to fulfill the following requirements. The platform specific providers have to be portable to other platforms. The port of the providers to another platform has to be as cost-saving as possible. Therefore it is necessary to define platform independent interfaces on a very low level. That means the data gathering has to be as close at the resource as possible. A management application needs to trust the behavior of a provider. This implies that error messages from different platforms have the same meaning.

It exist three different types of provider interfaces. Each one represents a certain capability of a class /association.

- Instance
- Association
- Method

The **instance interface** is responsible for enumerating the available resource entities and performing actions on these instances. The following interfaces must be implemented by an instance provider:

- Cleanup()
- EnumInstanceNames()
- EnumInstances()
- GetInstance()
- SetInstance()
- CreateInstance()
• DeleteInstance()
• ExecQuery()

The **association interface** represents the knowledge about the relations certain resource entities have to each other. The following interfaces must be implemented by an association provider:

• AssociationCleanup()
• Associators()
• AssociatorNames()
• References()
• ReferenceNames()

The **method interface** is responsible for executing extrinsic methods on a certain class or instance, for example restarting the operating system. The following interfaces must be implemented by an method provider:

• MethodCleanup()
• InvokeMethod()
• DeActivateFilter()
• MustPoll()

CIM Client Tools

Below is the list of freeware tools that can be used to communicate to SP-X – CIM stack

1. WinRM
2. WSMAN CLI
3. wbemcli

**WINRM Request:**

**Enumerate:**

The format of the WinRM Enumerate request is:

```
```

Let us take the example of SP_ComputerSystem. The Winrm Enumerate request on SP_ComputerSystem will look like:

```
```
Get:

The format of the WinRM Get request is:

```
```

Let us take the example of SP_ComputerSystem. The WinRM Get request on SP_ComputerSystem will look like:

```
```

WSMAN CLI Request:

Enumerate:

The format of the Enumerate request is:

```
```

Let us take the example of SP_ComputerSystem. The wsmancli Enumerate request on SP_ComputerSystem will look like:

```
```

Get:

The format of the Get request is:

```
```

Let us take the example of SP_ComputerSystem. The wsmancli Get request on SP_ComputerSystem will look like:
wsmancli get 'http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/SP_ComputerSystem?
Name="IPMI Controller 32",CreationClassName="SP_ComputerSystem"' -u root -p superuser -y
basic -b http://root:superuser@10.0.3.204:80/wsman -N root/cimv2 -m 256 -M objepr -o –R
**WBEMCLI Request:**

**Enumerate:**

The general format is

```
wbemcli ei http:// [USERNAME]:[PASSWORD]@[IPAddress]:5988/[NAMESPACE]:[CIM_CLASSNAME] -nl
```

Example for SP_ComputerSystem Class

```
wbemcli ei http://root:superuser@10.0.3.204:5988/root/cimv2:SP_ComputerSystem
```

**Get:**

The general format is

```
wbemcli gi http:// [USERNAME]:[PASSWORD]@[IPAddress]:5988/[NAMESPACE]:<CIM_CLASSNAME>.{key prop[.....]} -nl
```

Example for SP_ComputerSystem Class

```
wblemcli gi 'http://root:superuser@10.0.3.204:5988/root/cimv2:SP_ComputerSystem.Name="IPMI Controller 32",CreationClassName="SP_ComputerSystem"' -nl
```
One of the powerful tools in IPMI is Serial Over LAN (SOL) which provides serial line access over the management LAN. The baseboard management controller (BMC) microcontroller embedded on the server motherboard does this by redirecting information destined for the serial port over to the LAN. With SOL console redirection system administrators can remotely view the text-based console on their remote servers from anywhere and perform any task that doesn’t require a GUI.

Transporting serial data over IP networks using telnet, serial over IP, SOL and the likes is the way forward for server serial communications. Just as the KVM functions in embedded service processors is displacing the need for external KVM appliances, so the SOL capability of BMCs and console redirection in service processors is reducing the need for serial console servers for server console management.
Index

Absolute Mode, 48
Active Directory, 36, 37, 38, 39
ActiveX Console, 25
Add User, 78, 79, 80
Audit Log, 76, 77
Automatically synchronize, 52
Bind DN, 44
Bind Password, 44
Cancel, 38, 39, 74, 80, 93
cd Verb:, 117
CD-ROM Media redirection, 111
CIM, 128
CIM Client Tools, 130
Clear All Event, 33
Configuration, 22, 35, 41, 42, 50, 51
Configuration Group, 35
Console Redirection, 84
Console Redirection Menu, 86
create verb, 123
Current Certificate, 74
Current Privacy Key, 74
Dashboard, 22, 24, 25, 85
Date, 3, 52, 53
Delete User, 78, 80
delete verb, 122
Device Information, 25
Display option, 125
DNS, 40
Domain Name, 37, 38, 39, 40, 41, 42
Domain Settings, 41
dump verb, 123
Event Log, 14, 28, 31, 32, 33, 34
Event log Category, 33
Examine option, 125
Exit, 86, 119, 127
exit Verb, 118
Features, 14
File Size, 76, 77
Filter Type, 33
Firmware Update, 97
Full Screen, 86
Hard Disk Drive Media redirection, 112
Help, 86, 94, 119, 126
HELP, 23, 120
Help option, 126
help verb, 119
IP Address, 38, 41, 44, 45, 50, 65, 75, 106, 110, 131
IPv4 Address, 25, 50, 51, 69
IPv6 Settings, 51
Java Console, 25, 84, 85, 89, 93, 95
Keyboard, 86, 87, 89, 92, 104
KVM Encryption, 67
LDAP, 43
Live Widget, 31
load verb, 123
Log Out, 99
Log Type, 76
Logout, 23
MÁC Address, 25, 50
Machine Name, 69, 71
Maintenance, 22, 97, 98
Maintenance Group, 97
Media, 14, 67, 68, 86, 90, 91, 93, 106, 107, 108, 109, 111, 112
Media Encryption, 67, 68
Menu Bar, 22
Modify User, 78, 80
Mouse, 48, 49, 86, 88, 89
Mouse Mode, 48
Network, 50
Network Information, 25
Network Privilege, 78, 79
New SSK Key, 79
New SSL Certificate, 74
NTP, 52
NTP Server, 52, 53
Options, 20, 37, 86, 89, 127
Output option, 124
Overview, 12
Password, 19, 20, 21, 44, 45, 70, 71, 79, 80, 107, 110
Pause redirection, 86
Port, 44, 45, 65, 66, 69, 71, 106, 110, 128
Print, 23
Profiles supported, 128
Quick Button and Logged-in User, 22
Quick Buttons, 95
RADIUS, 64
Refresh, 23, 52, 53, 86
Relative Mode, 48
Remote Control, 22, 25, 83, 85, 96
Remote Session, 67
Reset, 42, 45, 48, 51, 53, 65, 66, 67, 68, 70,
71, 77, 96, 119
reset verb, 122
Restore Factory Defaults, 98
Resume Redirection, 86
Role Group, 37, 39
Rotate Count, 76, 77
Save, 38, 39, 41, 42, 45, 48, 51, 53, 65, 66,
67, 68, 70, 71, 77
Search base, 44
Secret, 65, 66
Secure Socket Layer, 74
Sender Address, 69, 71
Sensor Monitoring, 25
Sensor Readings, 28, 29, 30
Sensor Type (drop down menu), 30
Server Address, 38, 65, 66, 76, 77
Server Health, 22, 28, 29, 32, 34
Server Health Group, 28
Server Power Control, 96
set verb, 120
show verb, 117
Simple Mail Transfer Protocol, 69
SMASHCLP, 115
SMTP, 69
SMTP Server requires Authentication, 70,
71
SOL, 134
SOL tools, 134
SSL, 74
Standard CLP Verb Options, 124
Standard CLP Verbs, 117
start verb, 121
Starting SMASHCLP, 116
stop verb, 122
System and Audio Log, 28
System and Audit Log, 76
System Log, 76, 77
Time, 25, 33, 37, 38, 52, 53, 65, 66
Upload, 74, 75
User ID, 78
User management, 78
User Name, 19, 21, 70, 78, 79, 106, 110
Username, 19, 21, 70
UTC Offset, 52
version verb, 120
Video, 86, 93, 94
Video Record, 93
Virtual Media Attach Mode, 67
VMCLI (Virtual Media Command line
interface), 106
WBEMCLI Request, 133
WSMAN CLI Request, 131
YAFUFlash, 100
YAFUKCS, 104