Supermicro Update Manager

(SUM)

User's Guide

Revision 2.7.0

The information in this USER'S GUIDE has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

Manual Revision 2.7.0

Release Date: September 3rd, 2021

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2013-2021 by Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

Version History

Date	Rev	Description
July-02-2013	1.0	1. Created this document.
July-30-2013	1.0a	1. Revised the software description of SUM and SMCIPMITool.jar in *1.2.1 OOB Usage Requirements (Remote Management Server)*.
September-12-2013	1.1	1. Added in-band Usage related sections. 2. Changed the command LoadFactoryDefault to LoadDefaultBiosCfg.
October-02-2013	1.2	1. Added Get/Change DMI information capability. 2. Added multi-system usage for OOB channel. 3. Eliminated --me_type option for the in-band UpdateBios command. 4. In-band UpdateBios command supports X10 MB.
January-06-2014	1.2a	1. Required BMC firmware image and IPMI driver to be installed for all in-band commands except the UpdateBios command. 2. Required product key to be activated for all in-band commands except the UpdateBios command. 3. Added the summary of running multiple systems. 4. Added exit code 80. Description: Product key is not activated.
June-09-2014	1.3	Major revision with new management command groups. 1. Added BMC Management commands: GetBmcInfo, UpdateBmc, GetBmcCfg and ChangeBmcCfg. 2. Added System Checks commands: CheckAssetInfo, CheckSensorData and CheckSystemUtilization. 3. Added System Event Log commands: GetEventLog and ClearEventLog. 4. Added in-band-usage for ActivateProductKey command. 5. Added exit code 68. Description: Invalid BMC configuration text file.

		6. Added exit code 69. Description: Invalid asset information.
July-31-2014	1.4	1. Added Application commands: TpmProvision, MountIsoImage and UnmountIsoImage. 2. For X10 Intel® Xeon® Processor E5 v3/v4 Product Family platform, in-band update bios requires --reboot option. 3. Revised CheckSystemUtilization output message for HDD/Network. 4. Revise output message for CheckAssetInfo: Units format matches dmidecode outoput. 5. Added exit code 36. Required device does not exist. 6. Added exit code 37. Required device does not work. 7. Added notices for exit code when using in-band command with --reboot option through SSH connection.
February -06-2015	1.4a	1. Added a notice for in-band UpdateBios command for jumper-less solution: You should use default OS when multi-boot is installed. 2. Changed the TpmProvision command: cleartpm option should be used with --image_url option. 3. Added support for checking SFT-SUM and SFT-DCMS-SINGLE node product keys. 4. Added a notice for In-band UpdateBios command: The command will disable some functions in OS, but they will be recovered after OS reboot. 5. Added a notice for in-band UpdateBios using SSH connection: Change the timeout length for both SSH client and server site to be two times longer than the typical time length of execution. 6. Changed the name “Product Key” to “Node Product Key”. 7. Added exit code 11. Invalid command line data. 8. Added the notice of using the CheckSensorData command output. 9. Updated the CheckAssetInfo command output: adding the CPU version field and changing the name “Network Interface” to “Add-on Network

		Interface". 10. Added *Appendix C: Platform Feature Support Matrix*. 11. Added the OS architecture information in the CheckSystemUtilization command output message. 12. Added a reminder for In-band Windows driver setup.
July-23-2015	1.5	1. Added in-band support for BMC management commands: GetBmcInfo, UpdateBmc, GetBmcCfg, and ChangeBmcCfg. 2. Added in-band support for EventLog management commands: GetEventLog and ClearEventLog. 3. Added in-band support for CheckOOBSupport command. 4. Removed requirement of actool. 5. Removed JAVA environment requirement for all commands, except OOB UpdateBios and UpdateBmc commands. 6. Changed the ActivateProductKey command: supports 344 bytes node product key format. 7. Added Key management commands: QueryProductKey, ClearProdcutKey. 8. Added a BIOS management command: EditDmiInfo. 9. Added Appendix D Third-Party Software. 10. Added the log support when rare exceptions occurred. 11. Added exit code 12: Function access denied.
January-28-2016	1.6	1. Supported X11 platform. 2. Removed JAVA requirement. 3. Supported FreeBSD OS for FreeBSD 7.1 x86_64 or later. 4. Supported RHEL4 OS for RHEL4u3 x86_64 or later 5. Added auto-activation feature using credential files 6. Added --overwrite_cfg and --overwrite_sdr option for UpdateBmc command.

		7. In-Band UpdateBios supported MEDisabling feature which has similar procedure as original jumperless procedure that requires twice reboot. 8. Added HTTP image server support for MountIsoImage and TpmProvision commands. 9. Added exit code 38: Function is not supported. 10. Added Feature Toggled On information in CheckOOBSupport command output. 11. Third-Party Software: Removed ipmitool/Jline. Added openssl/libcurl. 12. In-Band jumperless procedure show full log path when twice reboot is needed. 13. Removed TAS from package. Added TAS requirement note.
August-03-2016	1.6a	1. Renamed the TPM ISO image file to 20151217. 2. Added troubleshooting for BMC FW web server being unreachable after BMC FW was updated. 3. Added the description of failure to install Client ME Windows driver on Server ME system. 4. Added the recommended usage of running the OOB UpdateBios command. 5. Added the requirements for using an OOB network.
January-06-2017	1.6b	1. Renamed the TPM ISO image file to 20161013. 2. Added two options: --no_banner to suppress output banner messages and --no_progress UI option to suppress output progress messages. 3. Renamed the command names GetDefaultBiosCfg and GetCurrentBiosCfg and deprecated the old commands GetDefaultBiosCfgTextFile and GetCurrentBiosCfgTextFile, respectively. 4. Added OOB support for the CMM management commands: GetCmmInfo, UpdateCmm, GetCmmCfg, and ChangeCmmCfg. 5. Modified the command In-band UpdateBios to not to require the --reboot option and removed the --manual_reboot option.

July-21-2017	1.7	1. Renamed the TPM ISO image file to TPM_1.2_20170410. 2. Added the Storage Management commands: GetRaidControllerInfo, UpdateRaidController, GetRaidCfg, ChangeRaidCfg, GetSataInfo and GetNvmeInfo. 3. Added support for Ipv6. 4. Added the option --lock to the command TpmProvision. 5. Revised the command format --image_url to TpmProvision. 6. Added support for TAS for FreeBSD. 7. Added support for B2 and K1 platforms. 8. Changed exit code 8 from "File does not exist" to "Cannot open file." 9. No support has been provided for B9 Intel® Xeon® processor E5-2600 product family platform since SUM 1.7.0. 10. RAID related commands are only licensed to SFT-DCMS-SINGLE key. 11. Supported Intel Atom® Processor C3000 Series platform. 12. Added the BBS boot priority function in a BIOS configuration file. 13. Added information about where the logs are stored 14. Supported Apollo platform. 15. Added *Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files*.
October-27-2017	2.0	1. Added HII support for the X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and the platforms of later versions. 2. Renamed the command GetCurrentBiosCfgTextFile to be GetCurrentBiosCfg. 3. Renamed the command GetDefaultBiosCfgTextFile to be GetDefaultBiosCfg. 4. Modified the command CheckAssetInfo to support for Add-on Network Interface and Onboard/Add-on PCI Devices. 5. Added "Appendix E. How to Change BIOS Configurations in XML Files".

		6. Added the option --preserve_setting for the command UpdateBios. 7. Added the TPM command options to support X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets platform. 8. Added support for H11 AMD EPYC platform. 9. Renamed the TPM ISO image file to TPM_1.3_20170802. 10. Add the option --skip_unknown for the command UpdateBios. 11. Added support for checking SFT-DCMS-SVC-KEY node product key. 12. Supported Debian OS for Debian 7 x86_64 or later. 13. Added exit code 155 description: IPMI received invalid data.
February-02-2018	2.0a	1. Added the option --skip_bbs for the command ChangeBiosCfg. 2. The CMM related commands do not require any license.
August-17-2018	2.1	1. Added the commands GetPsuInfo and UpdatePsu to manage the PSU firmware image. 2. Added the commandsGet TpmInfo and TpmManage to manage TPM. 3. Added exit code 76 - Invalid TPM provision table file. 4. Added the OEM FID feature. 5. Modified gsetting note. 6. Added 7u superblade note. 7. Removed limitation: For ATEN BMC FW, --overwrite_sdr and --overwrite_cfg have to coexist. 8. Added command SetBiosPassword. 9. Added exit code 13 - Invalid argument. 10. Added the option --rc_path
February-20-2019	2.2	1. Added thread_count usage in customizing SUM configurations section for multiple systems management. 2. Added the --tui option and introduction to TUI features.

		3. Modified the “CheckAssetInfo” command console output. 4. Added BMC extension version in BMC information. 5. Added an instruction on installing a certification file to BMC FW using ChangeBmcCfg command. 6. Updated instruction of applying credential files for auto-activation. 7. Added exit code 77 - Invalid SUMRC file. 8. Added exit code 109 - This operation is prohibited. 9. Added exit code 120 - Invalid Redfish response. 10. Added the option -f, to load file content as password. 11. Updated Platform Feature Support Matrix.
May-16-2019	2.3	1. Added the --show_multi_full option. 2. Added the SetBmcPassword and SetCmmPassword commands. 3. Changed the support policy of UpdatePsu. 4. Showed extra information when using the --showall option at GetBiosInfo. 5. Added LAN configurations notes to BMC settings update. 6. Added the --pw_file option for the SetBiosPassword command. 7. Added the --file_only option to multiple commands. 8. Added exit code 249 - Special action is required.
November-19-2019	2.4	1. Added the usage requirement and instructions for building Linux driver. 2. Added *Appendix H. How to Sign a Driver in Linux*. 3. Added descriptions of signing a driver in Linux. 4. Added the option --kcs to the command UpdateBios. 5. Added commands GetKcsPriv and SetKcsPriv. 6. Added *Appendix I. BMC/CMM Password Rule*. 7. Added the options --policy and --precheck.

		8. Added the introduction to the Policy Based Update feature.
June-12-2020	2.5	1. Removed the key management command: ClearProdcutKey. 2. Added the commands GetLockdownMode and SetLockdownMode. 3. Added *Appendix J. System Lockdown Mode Matrix*. 4. Added the command SecureEraseDisk. 5. Added support for the in-band mode of mountisoimage and unmountisoimage commands. 6. Added the command GetGpuInfo. 7. Added the information for JBOD mode in RAID configuration. 8. Added the commands for PSU Management: GetPowerStatus, SetPowerAction. 9. Added the commands for Applications : RawCommand, GetUsbAccessMode, SetUsbAccessMode. 10. Added *Appendix E.6 License Requirement Setting*. 11. Move platform feature support matrix to file PlatformFeatureSupportMatrix. 12. Renamed *Appendix C. Platform Feature Support Matrix* to *Appendix C. Known Limitations*. 13. Added the JSON key format and the option --key_file to the command ActivateProductKey. 14. Added the Redfish Host Interface usage to UpdateBios, UpdateBmc, ActivateProductKey and QueryProductKey commands. 15. Added the commands MountFloppyImage and UnmountFloppyImage. 16. Added the command SecureEraseRaidHdd. 17. Added the option --backup. 18. Added the option --forward. 19. Added the information about the node product key format to the

		command CheckOOBSupport. 20. Added the command GetMaintenEventLog. 21. Added the commands BiosRotManage and BmcRotManage. 22. Added the commands LoadDefaultBmcCfg and LoadDefaultCmmCfg. 23. Added the information about system's support for RoT features to the command CheckOOBSupport. 24. Added more options in the .sumrc file 25. Changed the example of running the command "QueryProductKey."
October-08-2020	2.5.1	1. Added the option --overwrite_ssl to the command UpdateBMC. 2. Added the new device type "Not TCG/SAT3 Supported" to the SecureEraseDisk command. 3. Updated the usage of TPM in the user's guide. 4. Removed the option --reboot from the command "BmcRotManage --action UpdateGolden."
December-24-2020	2.6.0	1. Added the commands GetCpldInfo and UpdateCpld. 2. Added the command LocateServerUid. 3. Added the commands GetBbpInfo, UpdateBbp, and CmmPowerStatus. 4. Added the commands GetPMemInfo and UpdatePMem. 5. Updated X12 BMC/CMM Password Rules in *Appendix I. BMC/CMM Password Rule*. 6. Added a notice to the commands GetBmcCfg and ChangeBmcCfg. 7. Added the command ServiceCalls. 8. Added new descriptions to *1.1 Features*. 9. Added the options --overwrite_sdr and --overwrite_ssl to the command UpdateCMM. 10. Added the command GetHostDump. 11. Added the command ClearMaintenEventLog.

		12. Added the option --post_complete to the commands to check POST status after system reboot: ChangeBiosCfg, LoadDefaultBiosCfg, ChangeDmiInfo, SetBiosPassword, ClearEventLog, SecureEraseDisk, UpdateBios, SetLockdownMode, SetPowerAction, UpdateRaidController, BiosRotManage and UpdateCpld. 13. Added Ipv6 address usage to the MountIsoImage command. 14. Added the option --controller to the commands GetRaidControllerInfo and UpdateRaidController. 15. Added the Redfish Host Interface usage to the commands GetRaidControllerInfo and UpdateRaidController. 16. Added support for Broadcom 3008 and Marvell SE9230 to the command GetRaidControllerInfo. 17. Added support for Marvell SE9230 to the command UpdateRaidController. 18. Added the commands GetBladePowerStatus and SetBladePowerAction. 19. Added the command TimedBmcReset.
September-03-2021	2.7.0	1. Updated the supported Windows version. 2. Updated the steps and descriptions of building a Linux driver. 3. Added support for Marvell SE9230 to the GetRaidCfg and ChangeRaidCfg commands.

Contents

Version History 3

Contents 13

1 Overview 23

1.1 Features 23

1.2 Operations Requirements 26

1.2.1 OOB Usage Requirements (Remote Management Server) 26

1.2.2 OOB Usage Requirements (Network) 26

1.2.3 OOB Usage Requirements (Managed Systems) 27

1.2.4 In-Band Usage Requirements 29

1.2.5 Additional In-Band Usage Requirements 31

1.3 Typographical Convertions 32

2 Installation and Setup 33

2.1 Installing SUM 33

2.2 Setting Up OOB Managed Systems 34

2.2.1 Installing the TAS Package 34

2.3 Setting Up In-Band Managed Systems 36

2.3.1 Building a Linux Driver 36

2.3.2 Signing a Driver in Linux 36

3 Licensing Managed Systems 37

3.1 Receiving Node Product Keys from Supermicro 37

3.2 Activating Managed Systems 38

3.3 Auto-Activating Managed Systems 38

4 Basic User Interface 40

4.1 Customizing SUM Configurations 58
4.2 SUM Log Design 61
4.3 Format of BIOS Settings Text File 63
4.3.1 An Example of BBS Boot Priority 64
4.4 BIOS Settings XML File format 66
4.5 DMI Information XML File format 69
4.6 BMC Configuration XML File format 71
4.7 RAID Configuration XML File format 73
4.8 CMM Configuration XML File Format 88
4.9 TUI 90
4.9.1 TUI General Reminders 91
4.9.2 BIOS TUI Configuration 92
4.10 Redfish Host Interface 101
4.10.1 Using Redfish Host Interface 101
4.10.2 Supported Commands 101
5 Managing a Single System 102
5.1 Key Management for a Single System 103
5.1.1 Activating a Single Managed System 103
5.1.2 Querying the Node Product Keys 104
5.2 System Checks for a Single System 106
5.2.1 Checking OOB Support 106
5.2.2 Checking Asset Information (OOB Only) 107
5.2.3 Checking Sensor Data (OOB Only) 118
5.2.4 Checking System Utilization (OOB Only) 119
5.2.5 ServiceCalls 122

5.3 BIOS Management for a Single System 129
5.3.1 Getting BIOS Firmware Image Information 129
5.3.2 Updating the BIOS Firmware Image 132
5.3.3 Receiving Current BIOS Settings 135
5.3.4 Updating BIOS Settings Based on the Current BIOS Settings 135
5.3.5 Receiving Factory BIOS Settings 139
5.3.6 Updating BIOS Settings Based on the Factory Settings 139
5.3.7 Loading Factory BIOS Settings 140
5.3.8 Receiving DMI Information 141
5.3.9 Editing DMI Information 141
5.3.10 Updating DMI Information 143
5.3.11 Setting Up BIOS Action 144
5.3.12 Setting Up a BIOS Administrator Password 145
5.3.13 Erasing the BIOS OA Key 146
5.3.14 Managing BIOS RoT Functions 147
5.4 BMC Management for a Single System 149
5.4.1 Getting BMC Firmware Image Information 149
5.4.2 Updating the BMC Firmware Image 151
5.4.3 Receiving BMC Settings 152
5.4.4 Updating BMC Settings 152
5.4.5 Installing BMC Certification 154
5.4.6 Setting Up a BMC User Password 155
5.4.7 Receiving the BMC KCS Privilege Level 156
5.4.8 Setting the BMC KCS Privilege Level 157
5.4.9 Loading Factory BMC Settings 158

5.4.10 Acquiring the BMC System Lockdown Mode 160
5.4.11 Setting the BMC System in Lockdown Mode 161
5.4.12 Managing BMC RoT Functions 161
5.4.13 Setting the BMC Reset Counter 163
5.5 Event Log Management for a Single System 164
5.5.1 Getting System Event Log 164
5.5.2 Clearing System Event Log 165
5.5.3 Getting System Maintenance Event Log 166
5.5.4 Getting Host Crash Dump Log 167
5.5.5 Clearing System Maintenance Event Log 168
5.6 CMM Management for a Single System (OOB Only) 169
5.6.1 Receiving CMM Firmware Image Information 169
5.6.2 Updating the CMM Firmware Image 170
5.6.3 Receiving CMM Settings 172
5.6.4 Updating CMM Settings 173
5.6.5 Setting Up a CMM User Password 174
5.6.6 Loading Factory CMM Settings 175
5.6.7 Receiving BBP Firmware Image Information 176
5.6.8 Updating the BBP Firmware Image 177
5.6.9 Getting Current Power Status of Blade System 178
5.6.10 Setting Power Status of Blade System 179
5.7 Applications for a Single System 181
5.7.1 Providing an ISO Image as a Virtual Media through BMC and File Server 181
5.7.2 Removing ISO Image as a Virtual Media 185
5.7.3 Mounting a Floppy Image as a Virtual Media from a Local Image File 186

5.7.4 Unmounting a Floppy Image as Virtual Media from the Managed System 187
5.7.5 Sending an IPMI Raw Command 188
5.7.6 USB Port Accessibility Control 189
5.7.7 Acquiring USB Port Access Mode (Inband Only) 190
5.7.8 Dynamically Controling USB Port Access Mode (Inband Only) 191
5.7.9 Controlling the UID of the Managed System 192
5.7.10 Booting into the ISO image from HTTP Server 193
5.8 Storage Management for a Single System 195
5.8.1 Getting RAID Firmware Image Information 195
5.8.2 Updating the RAID Firmware Image 197
5.8.3 Receiving RAID Settings 198
5.8.4 Updating RAID Settings 199
5.8.5 Getting SATA HDD Information (OOB Only) 200
5.8.6 Getting NVMe Information 201
5.8.7 Secure Erasing Hard Disks 202
5.8.8 Securely Erasing Hard Disks in LSI MegaRaid SAS 3108 RAID Controller 209
5.8.9 Getting PMem Firmware Image Information 217
5.8.10 Updating the PMem Firmware Image 219
5.9 PSU Management for a Single System 220
5.9.1 Getting PSU Information 220
5.9.2 Updating the Signed PSU Firmware Image Requested by OEM 221
5.9.3 Getting Current Power Status of Managed System 222
5.9.4 Setting Power Action of Managed System 223
5.10 TPM Management for a Single System 224
5.10.1 Getting TPM Information 225

5.10.2 Provisioning TPM Module 239
5.10.3 Enabling and Clearing TPM Module Capabilities 242
5.11 GPU Management 245
5.11.1 Getting GPU Information 245
5.12 CPLD Management 253
5.12.1 Getting CPLD Firmware Image Information 253
5.12.2 Updating the CPLD Firmware Image 255
6 Managing Multiple Systems (OOB Only) 256
6.1 Input Output Controls for Multiple Systems 258
6.1.1 File Input 258
6.1.2 File Output 258
6.1.3 Screen Output 259
6.1.4 Log Output 263
6.2 Key Management for Multiple Systems 265
6.2.1 Activating Multiple Managed Systems 265
6.2.2 Querying Node Product Key 266
6.3 System Checks for Multiple System 268
6.3.1 Checking OOB Support 268
6.3.2 Checking Asset Information 268
6.3.3 Checking Sensor Data 269
6.3.4 Checking System Utilization 269
6.3.5 ServiceCalls 270
6.4 BIOS Management for Multiple Systems 271
6.4.1 Getting BIOS Firmware Image Information 271
6.4.2 Updating the BIOS Firmware Image 271

6.4.3 Receiving Current BIOS Settings 272
6.4.4 Updating BIOS Settings Based on a Current Sample Settings 273
6.4.5 Receiving Factory BIOS Settings 274
6.4.6 Updating BIOS Settings Based on Factory Sample Settings 275
6.4.7 Loading Factory BIOS Settings 275
6.4.8 Receiving DMI Information 275
6.4.9 Editing DMI Information 276
6.4.10 Updating DMI Information Based on a Sample DMI Information 277
6.4.11 Setting BIOS Action 279
6.4.12 Setting BIOS Administrator Password 280
6.4.13 Managing BIOS RoT Funtions 280
6.5 BMC Management for Multiple Systems 282
6.5.1 Getting BMC Firmware Image Information 282
6.5.2 Updating the BMC Firmware Image 282
6.5.3 Receiving BMC Settings 283
6.5.4 Updating BMC Settings 284
6.5.5 Setting Up the BMC User Password 286
6.5.6 Receiving the BMC KCS Privilege Level 288
6.5.7 Setting the BMC KCS Privilege Level 288
6.5.8 Loading Factory BMC Settings 289
6.5.9 Acquiring the BMC System Lockdown Mode Status 290
6.5.10 Setting the BMC System Lockdown Mode 290
6.5.11 Managing BMC RoT Functions 291
6.5.12 Setting the BMC Reset Counter 291
6.6 Event Log Management for Multiple Systems 292

6.6.1 Getting System Event Log 292
6.6.2 Clearing System Event Log 292
6.6.3 Getting the System Maintenance Event Log 293
6.6.4 Getting Host Crash Dump Data Log 294
6.6.5 Clearing System Maintenance Event Log 295
6.7 CMM Management for Multiple Systems 296
6.7.1 Receiving CMM Image Information 296
6.7.2 Updating the CMM Firmware Image 297
6.7.3 Receiving CMM Settings 297
6.7.4 Updating CMM Settings 298
6.7.5 Setting Up a CMM User Password 299
6.7.6 Loading Factory CMM Settings 301
6.7.7 Receiving BBP Image Information 302
6.7.8 Updating the BBP Firmware Image 302
6.7.9 Getting Current Power Status of Blade System 303
6.7.10 Setting Power Status of Blade System 303
6.8 Applications for Multiple Systems 305
6.8.1 Providing an ISO Image as a Virtual Media through BMC and File Server 305
6.8.2 Removing ISO Image as a Virtual Media 306
6.8.3 Mounting a Floppy Image as Virtually from a Local Image File 307
6.8.4 Unmounting a Floppy Image as Virtually from the Managed System 308
6.8.5 Sending an IPMI Raw Command 309
6.8.6 Controlling the UIDs of Multiple Managed Systems 310
6.8.7 Booting into the ISO Image from HTTP Server 311
6.9 Storage Management for Multiple Systems 313

6.9.1 Getting RAID Firmware Image Information 313
6.9.2 Updating the RAID Firmware Image 313
6.9.3 Receiving RAID Settings 314
6.9.4 Updating RAID Settings 315
6.9.5 Getting SATA HDD Information 316
6.9.6 Getting NVMe Information 317
6.9.7 Securely-Erasing Hard Disks 318
6.9.8 Securely Erasing Hard Disks in LSI MegaRaid SAS 3108 RAID Controller 319
6.9.9 Getting PMem Firmware Image Information 321
6.9.10 Updating the PMem Firmware Image 322
6.10 PSU Management for Multiple Systems 323
6.10.1 Getting PSU Information 323
6.10.2 Updating the Signed PSU Firmware Image Requested by OEM 323
6.10.3 Getting the Current Power Status of the Managed System 324
6.10.4 Setting Power Action of Managed System 324
6.11 TPM Management for Multiple Systems 326
6.11.1 Getting TPM Information 326
6.11.2 Provisioning TPM Module 327
6.11.3 Enabling and Clearing TPM Module Capabilities 329
6.12 Policy-Based Update 332
6.12.1 Updating the Managed System 332
6.12.2 Format of Policy File 333
6.12.3 Matching Rules 338
6.12.4 Policy Actions 338
6.12.5 Cache Files 339

6.12.6 Error Warning 341
6.13 GPU Management for Multiple Systems 343
6.13.1 Getting GPU Information 343
6.14 CPLD Management for Multiple Systems 344
6.14.1 Getting CPLD Firmware Image Information (Multiple Systems) 344
6.14.2 Updating the CPLD Firmware Image (Multiple Systems) 345
Appendix A. SUM Exit Codes 346
Appendix B. Management Interface and License Requirements 350
Appendix C. Known Limitations 353
Appendix D. Third-Party Software 354
Appendix E. How to Change BIOS Configurations in XML Files 356
E.1 Numeric 356
E.2 CheckBox 357
E.3 Option 357
E.4 Password 359
E.5 String 360
E.5.1 File Upload 360
E.6 License Requirement 362
Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files 364
F.1 Introduction 364
F.2 Getting/Setting an XML Value (XML Element) 364
F.3 Getting/Setting an XML Value (XML Attribute) 365
Appendix G. Removing Unchanged BIOS Settings in an XML File 366
Appendix H. How to Sign a Driver in Linux 368
Appendix I. BMC/CMM Password Rule 372

I.1 X11/H11 and earlier platforms including H12 non-RoT systems 372
I.2 X12/H12 and later platforms except H12 non-RoT systems 373
I.3 CMM 374
Appendix J. System Lockdown Mode Table 375
Contacting Supermicro 378

1 Overview

The Supermicro Update Manager (SUM) can be used to manage the BIOS, BMC/CMM and RAID firmware image update (Broadcom 3108 and Marvell SE9230) and configuration update (except Marvell SE9230) for select Supermicro systems. In addition, system checks as well as event log management are also supported. Moreover, special applications are also provided to facilitate system management. To update configurations, you can edit system BIOS settings, DMI information, BMC/CMM configurations and RAID configurations from readable text files, as well as use this update manager to apply these configurations.

Two channels are possible for management: the OOB (Out-Of-Band) channel, i.e. communication through the IPMI interface, and the in-band channel, i.e. communication through the local system interfaces. By the OOB channel, most management commands (except the command "CheckSystemUtilization") can be executed independently of the OS on the managed system and even before the system OS is installed.

1.1 Features

- Command-line interfaced (CLI) and scriptable
- Independent from OS on managed systems (for OOB usage)
- Operates through OOB (Out-Of-Band) and in-band methods
- Supports concurrent execution of OOB commands on multiple systems through a system list file
- System Checks
  - Checks asset device information/health remotely
  - Checks if both BIOS and BMC firmware images support OOB functions
  - Checks system utilization remotely

- Checks sensor data remotely
- Sends notification of system status via e-mail

- Key Management
  - Activates node product keys.
  - Querys node product keys.
- BIOS Management
  - Pre-checks system board ID to prevent flashing the wrong BIOS firmware image
  - Supports readable text files of BIOS configuration in plain text or XML format
  - Supports readable DMI information text file to be edited
  - Updates basic input/output system (BIOS) ROM
  - Jumperless update of ME Flash Descriptor (FDT) region when locally update BIOS ROM
  - Updates BIOS configurations (settings)
  - Updates BIOS Administrator password
  - Updates DMI information
  - Supports Root-of-Trust (RoT) Management
  - Erases OA key of the managed system.
- BMC Management
  - Supports readable text files of BMC configuration in XML format
  - Updates BMC firmware image
  - Updates BMC configuration
  - Updates BMC password
  - Sets system lockdown mode
  - Sets KCS privilege levels (remotely only)
  - Supports Root-of-Trust (RoT) Management
- System Event Log
  - Retrieves and clears BMC and BIOS event logs
  - Retrieves and clears maintenance event logs
  - Dowloads the system crash dump status from BMC
- Remote CMM Management
  - Supports readable text file of CMM configuration in XML format
  - Updates CMM firmware image

- Updates CMM configuration
- Updates CMM password
- Updates BBP firmware image
- Controls the power status of CMM system

- Storage Management
  - Retrieves RAID image information from local firmware image or remote RAID controller
  - Updates RAID controller firmware image remotely
  - Supports the readable text files of RAID configuration in XML format
  - Updates RAID configuration remotely only
  - Retrieves SATA HDD information remotely only
  - Retrieves NVMe information remotely only
  - Securely erases an HDD on the managed system
  - Securely erases hard disks (HDD or SSD) in the LSI MegaRaid SAS 3108 RAID controller system
  - Updates the PMem with the given PMem file
  - Retrieves the PMem firmware image information from the local or remote firmware image file
- Applications
  - Provisions/clears the trusted platform module (TPM) (remotely only)
  - Gets Power status and sets power action
  - Updates PSU (Power Supply Unit) firmware images and gets PSU information from the system
  - Gets Graphics Processing Unit (GPU) status
  - Mounts/unmounts an ISO image file from SAMBA/HTTP-shared folder (remotely only)
  - Mounts/unmounts a floppy image file from a local drive
  - Supports IPMI raw commands
  - Supports USB Port accessibility control
  - Boots into an ISO image from the image file server
  - Controls the UID (User Identification) of the managed system
- CPLD Management
  - Updates CPLD firmware image

1.2 Operations Requirements

1.2.1 OOB Usage Requirements (Remote Management Server)

To run remote update operations, you must meet the following requirements:

System Requirements:

Environment	Requirements
Hardware	50 MB free disk space
	128 MB available RAM
	Ethernet network interface card
Operating System	Linux: Red Hat Enterprise Linux Server 4 Update 3 (x86_64) or later Linux: CentOS 4.3 (x86_64) or later Linux: Ubuntu 12.04 LTS (x86_64) or later Linux: Debian 7 (x86_64) or later Linux: SUSE Linux Enterprise Server 12 SP3 or later Windows: Windows Server 2008 (x64) or later FreeBSD: FreeBSD 11 (x86_64) or later

The software you should have in advance:

Program/Script	Description
SUM	The main program for SUM

1.2.2 OOB Usage Requirements (Network)

Below network communication protocol and ports are required for running OOB commands.

Command	Network Requirements
All OOB commands	RMCP+ protocol through IPv4/IPv6 UDP with port 623.
OOB commands UpdateBios, UpdateBmc, UpdateCmm and	In addition to RMCP+ protocol through IPv4/IPv6 UDP with port 623, HTTP or HTTPS protocol through IPv4/IPv6 with the port defined in BMC/CMM configuration is required. The

UpdateRaidController	default HTTP and HTTPS ports are defined as ports 80 and 443, respectively.

1.2.3 OOB Usage Requirements (Managed Systems)

SUM can remotely manage the selected Supermicro motherboards/systems. Before use, you must activate the node product key for the managed systems. For details, see *3 Licensing Managed Systems.*

In addition, both the BMC and BIOS firmware images must meet the following requirements.

Firmware Image	Requirements
BMC Version	X9 ATEN platform (SMT_X9): 3.14 or later X10 ATEN platform (SMT_X10): 1.52 or later X11 ATEN platform (SMT_X11): 1.00 or later X12 ATEN platform (SMT_X12): 1.00 or later H11 ATEN platform (SMT_H11): 1.28 or later H12 ATEN platform (SMT_H12): 1.00 or later X9 AMI platform (SMM_X9): 2.32 or later
CMM Version	ATEN platform (SMT_MBIPMI): 2.45 or later
BIOS Version	Version 2.0 or later for select X9 Intel® Xeon® processor E5-2600 product family and X10 Intel® Xeon® Processor E3-1200 v3 Product Family systems Version 1.0 or later for select X10 Intel® Xeon® Processor E5 v3/v4 Product Family/X11/H11/X12/H12 systems

The TpmProvision command requires TPM ISO files.

Program/Script	Description
TPM_1.3_20170802.zip	EFI/TPM_LOCK.ISO Image for TPM provision. ReleaseNote.txt Release note for TPM ISO images usage. TPM_Detect.ISO Image for detecting platform and TPM version.

The CheckSystemUtilization command requires additional packages to be installed on the managed system.

Program/Script	Description	Privilege Requirement
TAS_1.6.0_build.200415.zip	A Thin Agent Service (TAS) program to be installed on the managed systems. Collects utilization information on managed system and update information to BMC.	To install and execute, TAS needs the root privilege of the operating system running on the managed system.

Below OS and tools are pre-requisite for TAS to be installed successfully on the managed system.

OS	Supported OS List	Program/Script
Windows	Windows 2008 R2 SP1 Windows 2012 R2 Windows 2016	• .NET framework 3.5 • smartmontools 6.5-1 • NVMe vendor specific driver (only required for using the **nvme** function) • Windows patch "KB3033929"(only required for Windows Server 2008 R2 SP1) • Intel RST CLI tool 13.2.0.1016 and 13.2.x.xxxx RSTe driver (specify tool version to specify RSTe driver version) • sas3ircu 17.00.00.00
Linux	RHEL 6.5/6.6/6.10 RHEL 7.0/7.1/7.5 SLES 11 SP4 Ubuntu 14.04 LTS CentOS 6.5/6.9/6.10/7.5	• ethtool package 2.6.33 • openIpmi driver • smartmontools 6.5.x • glibc 2.12 • storcli 1.20.15 (for LSI 3108) • mdadm 4.0 (for RAID) • nmcli 0.8.1 • net-tools 1.60-110.el6-2 • lsscsi 0.23-2.el6 • lsblk 2.17.2 • sas3ircu 17.00.00.00
FreeBSD	10.1 release 11.1 release	• smartmontools 6.5.x • libc 7 • storcli 1.20.15 (for LSI 3108) • graid (starting with FreeBSD 9.1 for RAID) and geom_raid.ko • pciutils 3.5.2 • mfip.ko(for LSI MegaRAID SMART) • sas3ircu 17.00.00.00 • libconfig 1.7.2

The firmware image below is pre-requisite for TAS to run successfully on the managed system.

Firmware Image	Requirements
BMC Version	X10 ATEN platform (SMT_X10): 1.58 or later X11 ATEN platform (SMT_X11): 1.00 or later X12 ATEN platform (SMT_X12): 1.00 or later H11 ATEN platform (SMT_H11): 1.28 or later H12 ATEN platform (SMT_H12): 1.00 or later

1.2.4 In-Band Usage Requirements

With the use of in-band, SUM can perform BIOS/BMC/EventLog Management functions for selected Supermicro motherboards/systems. The managed system must meet the following requirements.

System Requirements:

Environment	Requirements
Hardware	50 MB free disk space
	128 MB available RAM
Firmware image	BIOS Version 3.0 or later for X9 Intel® Xeon® processor E5-2600 product family and X10 Intel® Xeon® Processor E3-1200 v3 Product Family select systems. BIOS Version 1.0 or later for X10 Intel® Xeon® Processor E5 v3/v4 Product Family/X11/H11/X12/H12 select systems.
Operating System	Linux: Red Hat Enterprise Linux Server 4 updates 3 (x86_64) or later. Linux: CentOS 4.3 (x86_64) or later Linux: Ubuntu 12.04 LTS (x86_64) or later Linux: Debian 7 (x86_64) or later Linux: SUSE Linux Enterprise Server 12 SP3 or later Windows: From Windows Server 2008 R2 SP1 (x64) to Windows Server 2019

	FreeBSD: FreeBSD 7.111 (x86_64) or later

Note: Though SUM can be run on Red Hat Enterprise Linux Server 4 updates 3 or later, several OS might not be supported by hardware. For the list of supported operating systems, please check the OS support list.

Execution Privilege Requirements:

Privilege	Description
SUM Execution Privilege	To execute in-band functions, SUM needs the root/Administrator privilege of the operating system running on the managed system.

The software you should get in advance:

OS	Program/Script	Description
Linux/Windows/FreeBSD	SUM	The main program for SUM
Windows	driver/phymem.sys driver/pmdll64.dll	Access physical memory and IO ports

Please contact Supermicro for any necessary drivers.

Note: For Windows Server 2008 R2 and Windows 7, Windows driver requires Windows patch #3033929.
https://docs.microsoft.com/en-us/security-updates/securityadvisories/2015/3033929
Click the link below to download the patch
https://www.microsoft.com/en-us/download/confirmation.aspx?id=46083

1.2.5 Additional In-Band Usage Requirements

For in-band commands (except for commands “GetBiosInfo” and “UpdateBios”), the managed system must have BMC firmware image and IPMI driver installed. The BMC firmware image should meet the following requirements.

Firmware Image	Requirement
BMC Version	X9 ATEN platform (SMT_X9): 3.14 or later X10 ATEN platform (SMT_X10): 1.19 or later X11 ATEN platform (SMT_X11): 1.00 or later X12 ATEN platform (SMT_X12): 1.00 or later H11 ATEN platform (SMT_H11): 1.28 or later H12 ATEN platform (SMT_H12): 1.00 or later X9 AMI platform (SMM_X9): 2.32 or later

The drivers you should get in advance:

OS	Program/Script	Description
Red Hat. Enterprise Linux Server 4u3 or later (x86_64)/Ubuntu 12.04 or later (x86_64)/ FreeBSD 11 or later (x86_64)	built-in IPMI driver	Sends/Receives data to/from BMC

If the Linux/FreeBSD OS does not have the built-in IPMI driver, you should install the following software:

Program/Script	Description
OpenIPMI.x86_64	IPMI driver for accessing BMC through its KCS interface

1.3 Typographical Convertions

This manual uses the following typographical conventions.

`Courier-New font size 10` represents Command Line Interface (CLI) instructions in Linux terminal mode.

Bold is used for keywords needing attention.

Italics is used for variables and section names.

<> encloses the parameters in the syntax description.`[shell]#` represents the input prompt in Linux terminal mode.

`[SUM_HOME]#` represents the SUM home directory prompt in Linux terminal mode.

| A vertical bar separates the items in a list.

2 Installation and Setup

2.1 Installing SUM

To install SUM in Linux/FreeBSD OS, follow these steps. Windows installation and usage is similar.

1. Extract the sum_x.x.x_Linux_x86_64_YYYYMMDD.tar.gz archive file.
2. Go to the extracted sum_x.x.x_Linux_x86_64 directory. Name this directory as “SUM_HOME”.
3. Run SUM in the SUM_HOME directory.

Linux Example:

```
[shell]# tar xzf sum_x.x.x_Linux_x64_YYYYMMDD.tar.gz

[shell]# cd sum_x.x.x_Linux_x86_64

[SUM_HOME]# ./sum
```

- **Note:** It is recommended that SUM tool with SUM release package should be used because binary files are required for certain commands.

2.2 Setting Up OOB Managed Systems

To setup OOB managed systems, follow these steps:

1. Connect the BMC/CMM to the LAN.
2. Update the BMC/CMM firmware image in the managed systems to support OOB functions (if the current version does not support it). Note that you can use the SUM UpdateBmc/UpdateCmm command to flash BMC/CMM firmware image even when BMC/CMM does not support OOB functions.
3. Flash the BIOS ROM to the managed systems to support OOB functions (if the current version does not support it). Note that you can use the SUM "UpdateBios" command (either in-band or OOB) to flash BIOS even when BIOS does not support OOB functions. However, when using an OOB channel, if the onboard BIOS or the BIOS firmware image does not support OOB functions, the DMI information (such as the MB serial number) might be lost after system reboot.
4. Install the TAS package on the OS of the managed system (for "CheckSystemUtilization" command only).

2.2.1 Installing the TAS Package

The TAS package (TAS_version_build.date.zip) can be acquired from Supermicro. Only Windows, Linux and FreeBSD platforms are supported. To install TAS, follow below steps.

1. Copy the TAS_version_build.YYMMDD.zip package to the operation system (OS) of managed system.
2. Extract the TAS_version_build.YYMMDD.zip archive file. Three archive files will be created, e.g., TAS_version_build.YYMMDD_Windows.zip/Linux.tar.gz/Freebsd.tar.gz, for Windows/Linux/FreeBSD systems. One additional readme file will be created. You can check the INSTALLATION section in the readme file or follow the steps below.
3. Install TAS pre-requisite tools listed in *1.2.3 OOB Usage Requirements (Managed Systems).*
4. For Windows systems,
   a. Extract the file TAS_version_build.YYMMDD_Windows.zip
   b. Select the correct system architecture. For x64 system, select folder 64.
   c. Run setup.bat
5. For Linux systems,

a. Extract the file TAS_version_build.YYMMDD_Linux.tar.gz

b. Select the correct system architecture.

c. Run install.sh

Example: for x86_64 Linux system

```
[shell]# tar xzf TAS_1.5.1_build.180202_Linux.tar.gz

[shell]# cd 64bit

[shell]# ./install.sh
```

6. For FreeBSD systems,

   a. Extract the file TAS_version_build.YYMMDD_Freebsd.tar.gz

   b. Run install

2.3 Setting Up In-Band Managed Systems

For Windows OS, no action is required. As a reminder, if the version of the currently installed Windows driver is old, SUM would stop TAS/SD5, load a new driver and restart TAS/SD5. For Linux OS, no action is required either, but if the BIOS item "Secure Boot" is enabled, the following actions must be taken to set up the Linux in-band managed systems. The first step is to build the Linux driver, and the second step is to sign the driver

2.3.1 Building a Linux Driver

To build the driver, install kernel-devel for their OS, then execute "make" under the SUM_HOME/driver/Source/Linux directory.

Syntax:

```
[shell]# make
```

2.3.2 Signing a Driver in Linux

After you have made arrangements for signing the driver (refer to *Appendix H. How to Sign a Driver in Linux*), and obtain the keys to execute the command in the driver folder.

Syntax:

```
[shell]# /lib/modules/$(uname -r)/build/scripts/sign-file sha256 <private key name>.priv <public key name>.der sum_bios.ko
```

For Kernel prior to 4.3.3, the command should run with perl.

Syntax:

```
[shell]# perl /lib/modules/$(uname -r)/build/scripts/sign-file sha256 <private key name>.priv <public key name>.der sum_bios.ko
```

Note: To generate the keys to run the command to sign a driver, run step 5 in *Appendix H. How to Sign a Driver in Linux*:

- **<private key name>**.priv: the generated private key file name.
- **<public key name>.**der: the generated public key file name.

3 Licensing Managed Systems

Each node is licensed by a product key. To access most SUM functions, it is required that a managed system activates the node product keys. To view a complete list of these functions, please refer to *Appendix B. Management Interface and License Requirements*. Product key activation is not required on the management server running SUM. The node product key is binding in the MAC address of the BMC LAN port. Two license key formats are supported: JSON and non-JSON. The JSON format supports all types of product keys. The non-JSON format includes these types: xxxx-xxxx-xxxx-xxxx-xxxx-xxxx for SFT-OOB-LIC and a 344-byte ASCII string for the other node product keys.

The following sections describe the steps for activation. First, you can receive the node product keys from Supermicro as in *3.1 Receiving Node Product Keys from Supermicro*. With these node product keys, you can then activate these systems as described in *3.2 Activating Managed Systems*. SUM also provided auto-activation methods for customer usage. For this usage please refer to *3.3 Auto-Activating Managed Systems*.

3.1 Receiving Node Product Keys from Supermicro

To receive node product keys from Supermicro, follow these steps:

1. Collect BMC MAC address and list them in one file, e.g., mymacs.txt.

Example:

```
003048001012
003048001013
003048001014
003048001015
```

2. Send this file (mymacs.txt) to Supermicro to obtain a node product key file (mymacs.txt.key). The node product key file includes the MAC address and node product key.

Example:

Non-JSON Format

```
003048001012;1111-1111-1111-1111-1111-1111-1111
003048001013;2222-2222-2222-2222-2222-2222-2222
003048001014;3333-3333-3333-3333-3333-3333-3333
```

JSON-Format

```
003048001015;{"ProductKey":{"Node":{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111112222222222222233333333333333ab
abababababababababababbabcdcdcdcdcdcdccdcdcddcdefefefefefefefeefefefefghghghghghghghghghgh"}}
```

3.2 Activating Managed Systems

To activate a single system, see *5.1.1 Activating a Single Managed System*. To simultaneously activate multiple systems see *6.2.1 Activating Multiple Managed Systems*.

3.3 Auto-Activating Managed Systems

For a new completely assembled system, its node product key can be activated while it is in production. It is strongly recommended that node product keys should be activated in this way. Please contact your sales representative for details.

However, in some cases, it is also possible to activate node product keys without running the command "ActivateProductKey." Follow these steps:

1. Collect the BMC MAC addresses of managed systems and list them in a text file, e.g., "mymacs.txt".
2. Send this file ("mymacs.txt") to Supermicro through your sales representative to obtain a credential file ("cred.bin").
3. Put the credential file in the "SUM_HOME/credential" directory on the system where the required SUM command is run.
4. SUM will auto-activate product keys from cred.bin after license-required commands are run on the managed systems.

Note: Auto-activation is not a site license.

4 Basic User Interface

SUM is a binary executable file written in the C++ language. Running this file on either Windows or Linux/FreeBSD is similar. In this document, only the examples of running on Linux are provided. To display the usage information, use this command:

```
[SUM_HOME]# ./sum
```

To display the usage information for each SUM command, use this syntax:

```
[SUM_HOME]# ./sum -h -c <command name>
```

Example:

```
[SUM_HOME]# ./sum -h -c UpdateBios
```

Usage Information

Options	Description or usage
-h	Shows help information.
-v	Displays the verbose output on the screen.
-i	<BMC/CMM IP address or host name> (case sensitive)
-l	<BMC/CMM system list file name>
-u	<BMC/CMM user ID>
-p	<BMC/CMM user password>
-f	<BMC/CMM user password file> Reads the first line of password file as password.
-c	<command name>
--no_banner	Hides the version and copyright banner.
--no_progress	Hides the progress message.
--journal_level	<set SUM journal level> (0: silent, 1: fatal, 2: error, 3: warning, 4: information, 5: debug, 6: verbose)
--journal_path	<set SUM journal path>

--rc_path	<set .sumrc file path>
--show_multi_full	Shows intermediate status of all managed systems. (For concurrent systems, only OOB managed systems are shown.)

System Check	
Commands	**Long options**
CheckOOBSupport	None
CheckAssetInfo **(OOB only)**	None
CheckSensorData **(OOB only)**	None
CheckSystemUtilization **(OOB only)** (TAS thin agent is required.)	None
ServiceCalls	**--file <file name>** Monitors the host with the given XML-style file listing system event logs and sensor data records.

Key Management	
Commands	**Long options**
ActivateProductKey	**-I Redfish_HI (Optional)** Uses Redfish Host Interface to activate the product key. (Only in-band usage is supported.) **--key <node product key value> (Optional)** Uses the node product key to activate the managed system. **--key_file <file name> (Optional)** Uses the node product key file to activate the managed system.
QueryProductKey	**-I Redfish_HI (Optional)** Uses Redfish Host Interface to query the key information. (Only in-band usage is supported.)

BIOS Management	
Commands	**Long options**
UpdateBios	**--file <file name>** Updates the BIOS with the given BIOS image file. **-I Redfish_HI (Optional)** Uses the Redfish Host Interface for in-band updates. (Only in-band usage is supported.)

	--reboot (Optional) Forces the managed system to reboot or power up after operation. This feature is supported since the X10 Intel® Xeon® Processor E5 v3/v4 Product Family platform. **--flash_smbios (Optional)** Overwrites and resets the SMBIOS data. This option is used only for specific purposes. Unless you are familiar with SMBIOS data, do not use this option. **--preserve_nv (Optional)** Preserves the NVRAM. This option is used only for specific purposes. Unless you are familiar with BIOS NVRAM, do not use this option. (Not available on X12 and later systems.) **--preserve_mer (Optional)** Preserves the ME firmware region. This option is used only for specific purposes. Unless you are familiar with ME firmware image, do not use this option. (Not available on X12 and later RoT systems.) **--kcs (Optional)** Updates BIOS through KCS. (Only in-band usage is supported.) **--preserve_setting (Optional)** Preserves BIOS configurations. This option is used only for specific purposes. Unless you are familiar with BIOS configurations, do not use this option. **--erase_OA_key (Optional)** Erases OA key. **--policy <policy XML file> (Optional)** Updates the BIOS based on the given policy file. (Only supported for multiple systems OOB usage.) **--precheck (Optional)** Works with option --policy. Note that this option only shows the parsing results without updating BIOS. **--backup (Optional)** Backs up the current BIOS image. (Only supported by the RoT systems.) **--forward (Optional)** Confirms the Rollback ID and upgrades to the next revision. (Only supported by the X12/H12 and later platforms except the H12 non-RoT systems.) **--post_complete (Optional)**

	Waits for the managed system's POST to complete after reboot. **--clear_password (Optional)** Clears BIOS password. **--erase_secure_boot_key (Optional)** Erases secure boot key. **--reset_boot_option (Optional)** Resets BIOS boot configurations.
GetBiosInfo	**--file <file name> (Optional)** Reads BIOS information from an input BIOS image file. **--showall (Optional)** Prints the BIOS version, BIOS revision and BIOS OEM FID information. **--file_only (Optional)** Works with --file, and only reads BIOS information from the input image file.
GetDefaultBiosCfg	**--file <file name> (Optional)** Saves the BIOS configuration to a file. Prints the default factory BIOS configuration on the screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file. **--uefi_boot (Optional)** Generate the BIOS configuration with UEFI Boot instead of Fixed Boot.
GetCurrentBiosCfg	**--file <file name> (Optional)** Saves the BIOS configuration to a file. Prints the current BIOS configuration on the screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file. **--tui (Optional)** Edits BIOS configuration with text-based user interface. **--compact (Optional)** Generates a compact version of the BIOS configuration containing only the settings that have been changed in the text-based user interface. **--uefi_boot (Optional)** Generate the BIOS configuration with UEFI Boot instead of Fixed Boot.

ChangeBiosCfg	**--file <file name>** Updates the BIOS with the given configuration file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each BIOS individually with the corresponding configuration file. **--skip_unknown (Optional)** Skips the unknown settings or menus in the BIOS configuration file. **--skip_bbs (Optional)** Skips the BBS-related menus in the BIOS configuration file. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot. **--skip_boot_option (Optional)** Skips the UEFI Boot menu in the BIOS configuration file.
LoadDefaultBiosCfg	**--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot. **--clear_bios_eventlog (Optional)** Clears the BIOS event log.
GetDmiInfo	**--file <file name> (Optional)** Saves the DMI information to a file. Prints the DMI information on the screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
EditDmiInfo	**--file <file name>** The DMI information file to be edited (or created if it does not exist). **--item_type <item type>** Specifies the item type. **--item_name <item name>** Specifies the item name.

	--shn <short name> Specifies the item in short name format. **--value <assignment value>** Assigns the value to the item. **--default** Assigns the default value to the item. Notes: • Either [--item_type, --item_name] or [--shn] is required. Either [--value] or [--default] is required.
ChangeDmiInfo	**--file <file name>** Updates the DMI information with the given text file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each piece of DMI information with the corresponding text file individually. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
SetBiosAction	**--BBS <yes/no>** Shows/hides the settings related to BBS priority. Selecting yes will show the settings related to BBS priority and selecting no will hide them. **--reboot (Optional)** Forces the managed system to reboot or power up after operation.
SetBiosPassword	**--new_password <new password> (Optional)** Sets the new BIOS Administrator password. **--confirm_password <confirm password> (Optional)** Confirms the new BIOS Administrator password. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--pw_file <Password File> (Optional)** The specified file path to read the new password. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.

	--cur_pw_file <Current Password File> (Optional) The specified file path to read the current password.
EraseOAKey	**--reboot (Optional)** Forces the managed system to reboot or power up after operation.
BiosRotManage	**--action <action>** Sets action to: 1 = GetInfo 2 = UpdateGolden 3 = Recover **--reboot (Optional)** Works with --action UpdateGolden and Recover. Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system POST to complete after reboot.
BMC Management	
Commands	**Long options**
UpdateBmc	**--file <file name>** Updates the BMC with the given BMC file. **-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band updates. (Only in-band usage is supported.) **--overwrite_cfg (Optional)** Overwrites the current BMC configuration using the factory default values in the given BMC image file. **--overwrite_sdr (Optional)** Overwrites current BMC SDR data. For AMI BMC FW, it must use the --overwrite_cfg option as well. **--overwrite_ssl (Optional)** Overwrites current BMC SSL configuration. (Only supported by X12/H12 and later platforms except for H12 non-RoT systems.) **--backup (Optional)** Backs up the current BMC image. (Only supported by the RoT systems.) **--forward (Optional)** Confirms the Rollback ID and upgrades to the next revision. (Only supported by X12/H12 and later platforms except for H12 non-RoT systems.) **--boot_check (Optional)** Checks if BMC boots up in 16 minutes after update. (Only supported on X12/H12 and later platforms except for H12 non-RoT systems.)

GetBmcInfo	**--file <file name> (Optional)** Reads the BMC information from the input BMC image file. **--file_only (Optional)** Works with --file, and only reads BMC information from the input image file.
GetBmcCfg	**-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band get BMC configuration. (Only in-band usage is supported.) **--file <file name> (Optional)** Saves the configuration to a file. Prints the BMC configuration on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
ChangeBmcCfg	**--file <file name>** Updates the BMC with the given configuration file. **-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band change BMC configuration. (Only in-band usage is supported.) **--individually (Optional)** Updates each BMC with the corresponding configuration file individually.
SetBmcPassword	**--user_id <user ID>** Enters the BMC user ID. **--new_password <new password>** Sets the new BMC user password. **--confirm_password <confirms password>** Confirms the new BMC user password. **--pw_file <password file>** The specified file path to read the new BMC user password.
GetKcsPriv	None
SetKcsPriv **(OOB only)**	**--priv_level <KCS privilege level>** Sets KCS privilege with level. 1 = Call Back 2 = User 3 = Operator 4 = Administrator
GetLockdownMode	None
SetLockdownMode	**--reboot**

	Forces the managed system to reboot or power up after operation. **--lock <yes/no>** <yes/no> Locks/Unlocks the managed system. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
LoadDefaultBmcCfg	**--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--clear_user_cfg** Clears user configuration. **--preserve_user_cfg** Preserves user configuration. **--load_unique_password** Loads the unique BMC password. **--load_default_password** Loads the default BMC password.
BmcRotManage	**--action <action>** Sets action to: 1 = GetInfo 2 = UpdateGolden 3 = Recover
TimedBmcReset	**--delay <BMC reset delay time>** Delay reset time. • Note: Delay time must be set within 1 to 60 minutes.
System Event Log	
Commands	**Long options**
GetEventLog	**--file <file name> (Optional)** Saves the event log to a file. Prints the event log on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
ClearEventLog	**--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot. **--clear_bmc_eventlog (Optional)** Only clears the BMC event log. **--clear_bios_eventlog (Optional)** Only clears the BIOS event log.
GetMaintenEventLog	**--st <start time>**

	Enters the start time YYYYMMDD. **--et <end time>** Enters the end time YYYYMMDD. **--file <file name>(Optional)** Saves the maintenance event log to a file. Prints the maintenance event log on screen if the file-saving function is not available. **--count <maintenance log count >(Optional)** Enters the log count. If the count is equal to zero, the entire maintenance event log will display. **--overwrite(Optional)** Overwrites the output file.
ClearMaintenEventLog	None
GetHostDump	**--action <action>** Sets action to: 1 = CreateDump 2 = DeleteDump 3 = DirectDump **--file <file name> (Optional)** Saves the crash dump data in a file. **--overwrite (Optional)** Overwrites the output file.
CMM Management (OOB Only)	
Commands	**Long options**
UpdateCmm	**--file <file name>** Updates the CMM with the given image file. **--overwrite_cfg (Optional)** Overwrites the current CMM configurations, including network settings using the factory default values in the given CMM image file. This might cause the IPMI connection to be lost. **--overwrite_sdr (Optional)** Overwrites the current CMM SDR data. (Only supported by the "CSE-947HE2C-R2K05JBOD" system.) **--overwrite_ssl (Optional)** Overwrites the current CMM SSL configuration. (Only supported by the "CSE-947HE2C-R2K05JBOD" system.)
GetCmmInfo	**--file <file name> (Optional)** Reads the CMM information from an input CMM image file. **--showall (Optional)** Gets the BIOS and BMC information of the managed system.

	--file_only (Optional) Works with the option --file, and only reads CMM information from the input image file.
GetCmmCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the CMM configuration on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
ChangeCmmCfg	**--file <file name>** Updates the CMM with the given configuration file. **--individually (Optional)** Updates each CMM with the corresponding configuration file individually.
SetCmmPassword	**--user_id < user ID>** Enters the CMM user ID. **--new_password <new password>** Sets the new CMM user password. **--confirm_password <confirms password>** Confirms the new CMM user password. **--pw_file <password file>** The specified file path to read the new CMM user password.
LoadDefaultCmmCfg	**--clear_user_cfg** Clears user configuration. **--preserve_user_cfg** Preserves user configuration. **--load_unique_password** Loads CMM unique password. **--load_default_password** Loads CMM default password.
GetBbpInfo	**--file <file name> (Optional)** Reads the BBP information from an input BBP image file. **--file_only (Optional)** Works with the option--file, and only reads BBP information from the input image file.
UpdateBbp	**--file <file name>** Updates the BBP with the given image file. **--skip_check (Optional)**

	Skips checking the blade power status to force a BBP update.
GetBladePowerStatus	None
SetBladePowerAction	**--action <action>** Sets power action with: 0 = down 1 = up 2 = cycle 3 = reset 4 = accycle 5 = softshutdown **--blade <Blade Index>** Assigns the blade index. [A1-A14], [B1-B14] or "ALL". **--node <Node Index> (Optional)** Assigns node index. [1-4]
Applications	
Commands	**Long options**
MountIsoImage	**--image_url <URL>** The URLs to access the shared image file SAMBA URL: 'smb://<host name or ip>/<shared point>/<file path>' SAMBA UNC: '\\<host name or ip>\<shared point>\<file path>' HTTP URL: 'http://<host name or ip>/<shared point>/<file path>' **--id <ID> (Optional)** The specified ID to access the shared file. **--pw <Password> (Optional)** The specified password to access the shared file. **--pw_file <Password File> (Optional)** The specified file path to read password.
UnmountIsoImage	None
MountFloppyImage	**--file <file name>** Mounts the specified binary floppy file to the managed system.
UnmountFloppyImage	None
RawCommand	**--raw <raw command>** Input hex-value commands
GetUsbAccessMode **(Inband only)**	None

SetUsbAccessMode **(Inband only)**	**--panel <front/rear>** The panel to be set. **--enable** Dynamically enables the USB ports in the assigned panel. **--disable** Dynamically disables the USB ports in the assigned panel.
LocateServerUid	**--action <action>** Sets action to: 1 = GetStatus 2 = On 3 = Off
SetHttpBoot	**--boot_name <boot description>** Description for HTTP boot. **--boot_lan <boot lan port>** Enter the LAN port for HTTP boot. LAN port 1 is only supported on X11 series. **--reboot** Forces the managed system to reboot or power up after operation. **--boot_clean** Cleans all HTTP boot options. **--disable_hostname_check** Disables HTTPS Boot from checking the hostname of TLS certificates matches the hostname provided by the remote server. **--image_url <URL>** The URL to access the shared image file. URL format: 'http://<IPv4 or IPv6>/<shared point>/<file path>' or 'https://<IPv4 or IPv6>/<shared point>/<file path>' **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
Storage Management	
Commands	**Long options**
GetRaidControllerInfo	**-I Redfish_HI (Optional)** Uses Redfish Host Interface to query the firmware information. (Only in-band usage is supported.) **--file <file name> (Optional)** Reads the RAID controller firmware information from an input RAID image file. **--controller <Controller> (Optional)** <Broadcom/Marvell> Vendor of RAID controller. **--dev_id <DEVICE_ID> (Optional)** RAID controller device ID.

	--file_only (Optional) Works with --file, and only reads RAID controller information from the input image file.
UpdateRaidController	**--file <file name>** Updates the RAID controller with the given RAID file. **--controller <Controller> (Optional)** <Broadcom/Marvell> Vendor of RAID controller. **--dev_id <Device ID>** Devce ID of RAID controller. **-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band updates. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
GetRaidCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the RAID configuration on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file. **--controller <Controller> (Optional)** <Broadcom/Marvell> Vendor of RAID controller.
ChangeRaidCfg	**--file <file name>** Updates the RAID with the given configuration file. **--individually (Optional)** Updates each RAID with the corresponding configuration file individually. **--controller <Controller> (Optional)** <Broadcom/Marvell> Vendor of RAID controller.
GetSataInfo **(OOB only)**	None
GetNvmeInfo **(OOB only)**	**--dev_id <Device ID> (Optional)** NVMe device controller ID. Prints all NVMe information on the screen if the file-saving function is not available.
SecureEraseDisk	**--file <file name>** HDD serial number mapping file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation.

	--precheck (Optional) Only displays HDD status. **--action <action> (Optional)** Sets secure erase action to: 1 = SetPassword 2 = SecurityErase 3 = SecurityErasePWD 4 = SecurityErasePSID 5 = ChangePassword 6 = ClearPassword **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
SecureEraseRaidHdd	**--dev_id <Device ID>** A LSI MegaRaid SAS 3108 RAID controller ID for secure erase. **--enc_id <Enclosure ID>** Enclosure ID list or "ALL" in the LSI MegaRaid SAS 3108 RAID controller for secure erase. **--dsk_id <Disk ID>** Disk ID list or "ALL" in the LSI MegaRaid SAS 3108 RAID controller for secure erase. **--tsk_id <Task ID> (Optional)** Accesses the progress of a secure erase. **--sync (Optional)** Shows the current progress of the secure-erase operation of the LSI MegaRaid SAS 3108 RAID controller.
UpdatePMem	**-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band update. **--file <file name> (Optional)** Updates the PMem with the given PMem firmware file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--restore_default_fw (Optional)** Updates the PMem with BIOS built-in PMem firmware. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
GetPMemInfo	**-I Redfish_HI (Optional)** Uses Redfish Host Interface to query the firmware information. (Only in-band usage is supported.) **--file <file name> (Optional)** Reads the PMem information from an input PMem image file.

	--file_only (Optional) Works with --file, and only reads PMem information from the input image file.
PSU Management	
Commands	**Long options**
GetPsuInfo	None
UpdatePsu	**--file <file name>** PSU firmware file **--address** PSU module address in HEX format (The PSU module slave address is obtained from the command GetPSUInfo.)
GetPowerStatus	None
SetPowerAction	**--action <action>** Sets power action with: 0 = up 1 = down 2 = cycle 3 = reset 4 = softshutdown 5 = reboot **--interval <time interval> (Optional)** Sets the power cycle interval in seconds. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
TPM Management	
Commands	**Long options**
TpmProvision **(OOB only)**	**--reboot** Forces the managed system to reboot or power up after operation. **--image_url <URL>** The URLs to access the shared image file. SAMBA URL: 'smb://<host name or ip>/<shared point>/<file path>' SAMBA UNC: '\\<host name or ip>\<shared point>\<file path>' HTTP URL: 'http://<host name or ip>/<shared point>/<file path>' **--lock <yes>** Locks the TPM module. **--id <ID> (Optional)** The specified ID to access the shared file. **--pw <Password> (Optional)** The specified password to access the shared file. **--pw_file <Password File> (Optional)** The specified file path to read password.

	--cleartpm (Optional) Clears the ownership of the TPM module and restores the relevant TPM BIOS settings.
GetTpmInfo	**--showall (Optional)** Prints the NV data and the capability flags (if applicable) of the trusted platform module.
TpmManage	**--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--clear_and_enable_dtpm_txt (Optional)** Clears dTPM ownership and activates dTPM/TXT. **--clear_dtpm (Optional)** Clears dTPM ownership and disables dTPM for TPM 1.2. Clears dTPM ownership for TPM 2.0. **--enable_txt_and_dtpm (Optional)** Enables TXT and dTPM. **--clear_and_enable_dtpm (Optional)** Clears dTPM ownership, disables dTPM (for TPM 1.2 only) and activates dTPM. **--disable_dtpm (Optional)** Disables dTPM. **--disable_txt (Optional)** Disables TXT. **--provision (Optional)** Launches the trusted platform module provision procedure. **--table_default (Optional)** Uses the default TPM provision table. **--table <table name> (Optional)** Uses the given customized TPM provision table file.
GPU Management	
Commands	**Long options**
GetGpuInfo	**--showall** Prints the FRU information on GPU baseboard of the managed system.
CPLD Management	
Commands	**Long options**
GetCpldInfo	**-I Redfish_HI (Optional)** Uses Redfish Host Interface to query the firmware information. (Only in-band usage is supported.) **--file <file name> (Optional)** Reads the CPLD information from an input CPLD image file. **--file_only (Optional)**

	Works with --file, and only reads CPLD information from the input image file.
UpdateCpld	**--file <file name>** Updates the CPLD with the given CPLD image file. **--reboot** Forces the managed system to reboot or power up after operation. **-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band update. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.

Notes:

- During execution, DO NOT remove the AC power on the managed system.
- DO NOT flash BMC and BIOS firmware images at the same time.
- To execute SUM, use either the relative path method, e.g. ./sum or absolute path method, e.g. /opt/sum_x.x.x_Linux_x64/sum in script file or shell command line.
- In Windows, use “double quotes” to enclose a parameter when needed.
- DO NOT update firmware image and configuration at the same managed system concurrently by in-band and OOB method.
- Before running the OOB UpdateBios command, it is recommended that the managed system is shut down first.
- By default, the command options are case insensitive. For in-band usage, simply ignore the -l, -i, -u, -p and -f options.
- Use the -p option or -f option to assign a password. These two options cannot be used together.
- For concurrent execution of OOB commands for managing multiple systems, use the -l option. For details on how to manage multiple systems, refer to *6 Managing Multiple Systems (OOB Only)*.
- When a command is executed, it will be recorded in *sum.log*. In addition, when rare exceptions occur in BMC/CMM/RAID configurations get/set commands, timestamp logs will be created. If the folder “/var/log/supermicro/SUM” exists, the logs will be stored there. Otherwise, they are stored in the same folder as $PWD in Unix-like OS or %cd% in Windows.
- For --reboot option in OOB usage, if target OS does support software shutdown and install X-window on RedHat OS, system will be forced to be powered off and then powered up. Please make sure that data is saved before the sum command is run. The Red Hat version decides if the software shutdown support can be enabled in console prompt.

If the system is configured to hibernate or sleep, the system may hang up when a server is rebooted. To avoid such a situation, run the following command in the target OS/system before you start to update BIOS:

```
gsettings set org.gnome.settings-daemon.plugins.power power-button-action nothing
```

- With the --post_complete option, the system will wait until the managed system POST is complete so that the managed system will be ready for the next OOB action.

4.1 Customizing SUM Configurations

Starting from SUM 2.1.0, two methods allow you to customize execution configurations, command options and .sumrc file. A command option is prior to a .sumrc file. In other words, a parameter in .sumrc file will be overwritten by a parameter in a command option. The default configuration will be applied only when nothing is assigned or valid in command option and .sumrc. The following table summarizes the configurable parameters:

Setting Name	Setting Value Sample	Description	Customized Methods
journal_level	[1]0: *silent*, 1: *fatal*, 2: *error*, 3: *warning*, 4: *information*, 5: *debug*, 6: *verbose*	Sets the journal level.	Both command options and .sumrc file
journal_path	[1]Linux: ~/journal/supermicro/sum/ [1]Windows: %HomePath%\journal\supermicro\sum\	Sets the journal output path. When the journal level is set to 0 (silent), this parameter will be invalid.	Both command option and .sumrc file
confirm_timeout	[1]300	[2]Sets the confirm flag polling timeout. The unit is second.	.sumrc file only
udp_timeout	[1]240	Sets the checking timeout for udp connection in seconds. The value should be between 1 and 240, inclusive.	.sumrc file only
thread_count	[1]50	[3]Set the thread count	.sumrc file only
multi_retry_count	[1]2	Set retry count for using concurrent system OOB.	.sumrc file only
ipv6_file_name_switch	[1]0: *disable*, 1: *enable*	Replace ':' with '-' when the file name contains an IPv6 address.	.sumrc file only
cache_path	[1]%WorkingDirectory%	[4]Sets the cache file path	.sumrc file only

		of ServiceCalls.	
https_port	[1]443	[5]Sets managed system https port	.sumrc file only
certificate	None	[6]Sets certificate files for verifying customized signed RoT firmware images	.sumrc file only

[1]Default configuration value

[2]When a file is uploaded to BIOS relayed by BMC, after reboot SUM will keep polling if the file is updated to BIOS successfully. If SUM can't receive "success" within the confirmed_timeout seconds, SUM will stop polling and show a message indicating that the file is "being updated". In this case, it denotes that the system requires more time to boot up. The confirm_timeout can be increased to make sure SUM receives a "success" message before timeout.

[3]SUM can limit its maximum concurrent executing count to avoid system overloading. The thread count in the .sumrc file can be adjusted to protect the system from overloading when SUM multiple node mode is executed. For example, if the thread count is set to 50, SUM will execute 50 working threads simultaneously.

[4] You cannot access any cache files on mounted file systems with the command ServiceCalls. Please make sure the target path is not in a mounted directory.

[5]The https port setting will be applied to OOB Redfish and Redfish Host Interface usage.

[6]The certificate file only supports X.509 in PEM and DER format.

There are three ways to specify the .sumrc file: command option --rc_path (highest priority), .sumrc file in the current directory (intermediate priority) and .sumrc in the user home directory (lowest priority). A user can rename sumrc.sample file to ".sumrc" in the current directory or move the file to the user home directory and rename to .sumrc based on user's requirements. Note that a .sumrc sample configuration file is bundled with SUM release package. An example is provided below.

```
# Please copy this file to the SUM execution directory or user home directory and rename to .sumrc
# The SUM execution directory will be read first and the user home directory have second priority.
# Please remove "#" to activate a customized configuration

# set SUM journal level
# 0: silent, 1: fatal, 2: error, 3: warning, 4: information, 5: debug, 6: verbose
```

```
#journal_level = 0

# set SUM journal path
# the following is an example path
#journal_path = /home/administrator/journal/supermicro/test

# set cache file path for ServiceCalls
#cache_path = /home/administrator/cache/supermicro/test

# set confirm flag polling timeout
# the unit is second
#confirm_timeout = 300

# sets the checking timeout for udp connection in seconds.
# The value should be between 1 and 240, inclusive.
#udp_timeout = 240

# set thread count
# thread_count = 50

# set retry count for concurrent system OOB usage
#multi_retry_count = 2

# set managed system https port
#https_port = 443

# replace ':' with '-' when file name contains an IPv6 address.
#ipv6_file_name_switch = 0

# set certificate file for verifying customized signed RoT firmware images
#certificate = /home/administrator/cert/public.cert
```

The syntax is "*name*=*value*". *name* is the parameter name defined by SUM and *value* is the parameter value that can be configured. If a parameter value is illegal, SUM will ignore it. By default, all the parameters in .sumrc are inactivated and "#" in front of the line may be removed to activate a parameter configuration.

Note: In Windows, please copy the SUM configuration file and rename it to .sumrc by Command Prompt.

4.2 SUM Log Design

While SUM commands are executed, log messages can be recorded for issue tracking and replication. Types of logs are detailed in this section.

- **Command usage history**

  When executing a SUM command, the executed command with options from console will be logged to a sum.log file automatically. The root cause of an issue may result from the previously executed command(s). History of command usages correlates combinations of executed commands, which also makes issue investigation easier.

- **Critical error log**

  When SUM encounters a critical error, the critical error message will be logged automatically. Just like system error logs, the critical error messages are always notable and require further actions.

- **Multiple-system log**

  When executing SUM command with multiple system modes (with -l option), a multiple system log will be generated automatically. The log summarizes all the running results for multiple systems. Running status (FAILED or SUCCESS), executing time and exit codes can be reviewed in this log.

- **Command execution journal**

  The journal is to record the footprint messages during the process of command execution. The severity levels rank from zero to six. The lowest level 0 (silent) generates no messages while the highest level 6 (verbose) generates the most messages. In addition to severity level, this journal is tagged with functional categories, for example, GENERIC, CURL and so on. Category GENERIC means messages do not fit to any particular category while category CURL includes message related curl library. With a functional category tag, journal can be filtered quickly and issue can be identified efficiently.

  By default, this journal is disabled (severity level 0) and it can be enabled by --journal_level option (higher priority) or .sumrc configuration (lower priority). Similarly, this journal will be created at the user home directory by default. Besides, if the output path is assigned in --journal_path option (higher priority) or .sumrc configuration (lower priority), the output path will be replaced.

The following table summarizes the properties of four sorts of logs.

Types of logs/ properties	Activation	Output path priorities
Command usage history	Always activated	1. Defined by the option --journal_path. The log exists inside the subfolder named as “History” in the folder path defined by the option --journal_path. 2. “/var/log/supermicro/SUM”. 3. $PWD in Linux or %cd% in Windows.
Critical error log	Always activated	1. Defined by the option --journal_path. The log exists inside the subfolder named as “Critical” in the folder path defined by the option --journal_path. 2. /var/log/supermicro/SUM. 3. $PWD in Linux or %cd% in Windows.
Multiple system log	Always activated	1. Defined by the option --journal_path. The log exists inside the subfolder named as “Multiple” in the folder path defined by the option --journal_path. 2. /var/log/supermicro/SUM. 3. The same directory as multiple list file.
Command execution journal	Activated by configuration	1. Defined by the option --journal_path. The log exists in the folder path defined by the option --journal_path. 2. Defined by .sumrc in the home directory. 3. ~/journal/supermicro/sum/ in Linux or %HomePath%\journal\supermicro\sum\ in Windows.

4.3 Format of BIOS Settings Text File

The BIOS settings file is designed to display the BIOS setup menu in text format for easier configurations. Each setup item consists of a variable, a value, options and dependency (if available). The example below shows how BIOS settings are displayed.

```
[Advanced|CPU Configuration|CPU Power Management Configuration]
Power Technology=01    // 00 (Disabled), *01 (Energy Efficient), 02 (Custom)
EIST=01               // 00 (Disabled), *01 (Enabled)        Power Technology =
"Custom"
Turbo Mode=01        // 00 (Disabled), *01 (Enabled)         Power Technology =
"Custom" and EIST = "Enabled"
C1E Support=01        // 00 (Disabled), *01 (Enabled)        Power Technology =
"Custom"
```

- A setup submenu is quoted by brackets. Setup items are next to the setup submenu.
- A variable (of one setup item) always stays on the left side of the "=" character.
- A value (of one variable) always stays on the right side of the "=" character.
- Annotated options (of one variable) are shown after "//" and "*" indicates the default option.
- A dependency (if available) will be separated from an option command by eight spaces. It indicates that the variable is visible and configurable when other variable(s) are set to a designated value.

In this example, the "*Power Technology"* item in the "*CPU Power Management configuration"* submenu is currently set to 01 for Energy Efficient (the default setting) and can be set to 00 for Disabled or 02 for Customer. The "*EIST"* variable is equal to 01 for Enabled (the default setting) and can be set to 00 when the "*Power Technology"* variable is set to 02 for Custom.

If the desired changes are limited to the "*Power Technology"* configuration, delete all except the two lines:

```
[Advanced|CPU Configuration|CPU Power Management Configuration]

Power Technology=01     // 00 (Disable), *01 (Energy Efficient), 02 (Custom)
```

Notes:

- You can remove unnecessary menu items (or variables) and their values still remain the same after an update.
- If all menu items are removed (or the file becomes empty), no configurations are changed.
- The Setup submenu is required for setting up the items.

4.3.1 An Example of BBS Boot Priority

On platforms before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, the command "SetBiosAction" is required to execute with the --BBS option set to yes, to activate the BIOS settings related to BBS Boot Priority.

This is an example of the boot order:

```
[Boot|Hard Disk Drive BBS Priorities]

HDD Boot Order #1=0000                  // *0000 (INTEL SSDSC2BB120G6), 0001
(SEAGATE ST3500418AS), 0002 (Disabled)

HDD Boot Order #2=0001                  // 0000 (INTEL SSDSC2BB120G6), *0001
(SEAGATE ST3500418AS), 0002 (Disabled)
```

In this example, "*HDD Boot Order #1"* is currently set to 0000 for INTEL SSDSC2BB120G6 and "*HDD Boot Order #2"* is set to 0001 for SEAGATE ST3500418AS. Boot orders could be swapped after changing BIOS configuration with the setting modified as below.

```
[Boot|Hard Disk Drive BBS Priorities]

HDD Boot Order #1=0001                  // *0000 (INTEL SSDSC2BB120G6), 0001
(SEAGATE ST3500418AS), 0002 (Disabled)

HDD Boot Order #2=0000                  // 0000 (INTEL SSDSC2BB120G6), *0001
(SEAGATE ST3500418AS), 0002 (Disabled)
```

The device is mapped with the boot order. Please note that after BIOS configurations are changed, the boot order indices (0000 and 0001 are boot order indices in the example above) and the mapped devices may be different. In this example, after ChangeBiosCfg took effect, GetCurrentBiosCfg will have the configuration as below:

```
[Boot|Hard Disk Drive BBS Priorities]

HDD Boot Order #1=0000                  // *0000 (SEAGATE ST3500418AS), 0001
(INTEL SSDSC2BB120G6), 0002 (Disabled)

HDD Boot Order #2=0001                  // 0000 (SEAGATE ST3500418AS), *0001
(INTEL SSDSC2BB120G6), 0002 (Disabled)
```

Notes:

- The settings of boot orders should not be the same except *Disabled*.
- GetDefaultBiosCfg command does not support these BBS settings for platforms before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets.

4.4 BIOS Settings XML File format

For easier configurations, the BiosCfg.xml file is designed to display the BIOS setup menu in XML format. An example below shows how this file demonstrates BIOS setup settings. Each setting consists of a default value and a current value.

```
<BiosCfg>
  <Menu name="IPMI">
    <Menu name="System Event Log">
      <Information>
        <Help><![CDATA[Press <Enter> to change the SEL event log
configuration.]]></Help>
      </Information>
      <Subtitle>Enabling/Disabling Options</Subtitle>
      <Setting name="SEL Components" selectedOption="Enabled" type="Option">
        <Information>
          <AvailableOptions>
            <Option value="0">Disabled</Option>
            <Option value="1">Enabled</Option>
          </AvailableOptions>
          <DefaultOption>Enabled</DefaultOption>
          <Help><![CDATA[Change this to enable or disable all features of System
Event Logging during boot.]]></Help>
        </Information>
      </Setting>
      <Subtitle></Subtitle>
      <Subtitle>Erasing Settings</Subtitle>
      <Setting name="Erase SEL" selectedOption="No" type="Option">
        <Information>
          <AvailableOptions>
            <Option value="0">No</Option>
            <Option value="1">Yes, On next reset</Option>
            <Option value="2">Yes, On every reset</Option>
          </AvailableOptions>
          <DefaultOption>No</DefaultOption>
          <Help><![CDATA[Choose options for erasing SEL.]]></Help>
```

```
          <WorkIf><![CDATA[  0 != SEL Components  ]]></WorkIf>
        </Information>
      </Setting>
    </Menu>
  </Menu>
</BiosCfg>
```

- The XML version is shown in the first line.
- The root table name is "*BiosCfg*". Its name tag pairs are *<BiosCfg>* and *</BiosCfg>*. All configurations of the root table are enclosed in between this name tag pair.
- The name tag pair *<BiosCfg>* is the root of all configurations and *<Menu>* is the only type of name tag pairs extending from *<BiosCfg>*.
- Each name tag pair *<Menu>* encloses name tag pairs *<Menu>*, *<Information>*, *<Setting>*, *<Subtitle>* and *<Text>*.
- <Information> is designed to display the name tag pairs *<Help>* and *<WorkIf>*. In addition, the setting-specific information is listed. For example, *<Setting>* with attribute 'name' as 'Option' has *<AvailableOptions>* and *<DefaultOption>* to indicate the selectable and default options, respectively. Any modification in the <Information> enclosure is unnecessary and NEVER takes effect.
- *<Setting>* is the only configurable part in the XML configuration. There are five supported setting types: 'Option', 'CheckBox', 'Numeric', 'String' and 'Password'. There are various *<Setting>* enclosures depending on the setting type. For instance, the accepted values for the setting 'Option' in *<SelectedOption>* enclosure are listed in *<AvailableOptions>* enclosure and any other setting values will cause exception thrown.
- *<Subtitle>* and *<Text>* are designed to indicate what is coming up next in the configuration.
- *<Help>* is designed to provide more explanations for menus and settings.
- *<WorkIf>* is designed to determine if the setting modification will take effect or not. If *<WorkIf>* enclosure is not shown, it implies the modified setting value will always take effect.

In this example XML file, the setting 'SEL Components' is enclosed in menu 'System Event Log'. The setting configuration will take effect only when *<WorkIf>* enclosure is evaluated as true (in this case, the setting 'BMC Support' is not equal to 0). If the setting value is modified in XML file and *<WorkIf>* enclosure is

evaluated as false, the warning messages will indicate that the changes will not take effect. Besides, if the setting value in *<SelectedOption> enclosure* is neither 'Enabled' nor 'Disabled', an exception will be thrown.

Moreover, two or more settings in the XML file might refer to the same variable in the BIN file. In this scenario, those setting values are expected to be consistent. For example, the setting 'Quiet Boot' in the menu 'Setup'->'Advanced'->'Boot Feature' and the setting 'Quiet Boot' in the menu 'Setup'->'Boot' are actually two different settings (different settings can have the same name). Indeed, they even refer to the same variable in the BIN file. If the setting values in these two questions are conflicted in the XML file, SUM will then throw an exception. For more details on usages, see *Appendix E. How to Change BIOS Configurations in XML Files*.

Notes:

- Unchanged settings can be deleted to skip the update.
- The XML version line and the root *<BiosCfg>* should not be deleted.
- The XML configuration contains extended ASCII characters, i.e. ©, ® and µ. It is REQUIRED to use a text editor that supports extended ASCII characters (ISO-8859-1 encoding). Otherwise, the extended ASCII characters might be lost after they are saved. It is suggested that Notepad++ in Windows and Vim in Linux could be used to view and edit the XML configuration.
- If garbled characters appear when viewing and editing the XML configurations with vim, it is likely that vim is incorrectly detecting the file's encoding. It is suggested that the setting into ~/.vimrc: set fileencodings=latin1,ucs-bom,utf-8,gb18030 should be added.
- For using tools to edit XML files, please refer to *Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files*.

4.5 DMI Information XML File format

DMI.txt is designed to display the supported editable DMI items in text format for easier update. An example below shows how this file demonstrates the DMI information items. Each item consists of an item name, a short name, a value, and comments.

```
[System]
Version                 {SYVS}    = "A Version"             // string value
Serial Number           {SYSN}    = $DEFAULT$                // string value
UUID                    {SYUU}    = 00112233-4455-6677-8899-AABBCCDDEEFF // 4-2-
2-2-6 formatted 16-byte hex values
    // Bytes[ 0-3 ]: The low field of the timestamp
    // Bytes[ 4-5 ]: The middle field of the timestamp
    // Bytes[ 6-7 ]: The high field of the timestamp (multiplexed with
    //               the version number)
    // Bytes[ 8-9 ]: The clock sequence (multiplexed with the variant)
    // Bytes[10-15]: The spatially unique node identifier
    // Byte Order  :
    //       UUID {00112233-4455-6677-8899-AABBCCDDEEFF} is stored as
    //       33 22 11 00 55 44 77 66 88 99 AA BB CC DD EE FF
```

- A DMI type is quoted by brackets. DMI information items are next to the DMI type.
- The name of a DMI information item is always followed by its short name.
- The item name and its short name stays at the left side of the "=" character.
- A short name is always enclosed by brackets.
- A value (of one information item) always stays at the right side of the "=" character.
- String values are enclosed by double quotation marks.
- $DEFAULT$ signature without double quotation marks is used to load default value for a string-valued item.
- There is no default value for non-string-value items.
- Do not use quotation marks for non-string-value items.

- The value type is always shown after a value and begins with "//".
- The value meanings for a non-string-value item are listed next to the item.

In this example, the "*Version"* DMI item belongs to the "*System"* DMI type with short name SYVS. It is string-value by "A Version" and can be changed to any other string value. For the "*Serial Number"* item, its value is set as $DEFAULT$. After updating the DMI information, the item value of the "*Serial Number"* will be reset to factory default. The *UUID* item is a specially formatted hex-value item. Its value meanings are explained next to it.

Notes:

- You can remove unnecessary DMI items so that its value will not be changed after an update.
- The DMI type is required for DMI items.
- Each item can be identified either by its short name or by the combination of its item type and item name.
- Any line begins with "//" will be ignored.
- A version number is included at the beginning of every DMI.txt file. This version number should not be modified because it is generated by SUM according to the BIOS of the managed system for DMI version control.

4.6 BMC Configuration XML File format

The BMC configuration file is designed to display the supported and editable BMC configuration elements in XML format for an easier update process. An example below shows how this file demonstrates the BMC configurable elements.

```
<?xml version="1.0"?>
<BmcCfg>
  <!--You can remove unnecessary elements so that-->
  <!--their values will not be changed after update-->
  <StdCfg Action="None">
    <!--Supported Action:None/Change-->
    <!--Standard BMC configuration tables-->
    <FRU Action="Change">
      <!--Supported Action:None/Change-->
      <Configuration>
        <!--Configuration for FRU data-->
        <BoardMfgName>Supermicro</BoardMfgName>
        <!--string value, 0~16 characters-->
      </Configuration>
    </FRU>
  </StdCfg>
  <OemCfg Action="Change">
    <!--Supported Action:None/Change-->
    <!--OEM BMC configuration tables-->
    <ServiceEnabling Action="Change">
      <!--Supported Action:None/Change-->
      <Configuration>
        <!--Configuration for ServiceEnabling-->
        <HTTP>Enable</HTTP>
        <!--Enable/Disable-->
      </Configuration>
    </ServiceEnabling>
  </OemCfg>
</BmcCfg>
```

- The XML version is shown in the first line.
- The root table name is "*BmcCfg*". Its name tag pair is *<BmcCfg>* and *</BmcCfg>*. All information belonging to the root table is enclosed between this name tag pair.
- There could be two direct children for the root table: "*StdCfg*" and "*OemCfg*".
- "*StdCfg*" and "*OemCfg*" could have child tables.
- Configurable elements are listed in the "*Configuration*" field of each child table.
- Each configurable element has a name tag pair. The element value is enclosed by its name tag pair.
- Comments could be given following any element or table name tag. Each comment is enclosed by "*<!--*" and "*-->*" tags. The supported usage of each element and table are shown in its following comments.
- Configuration tables could have an "*Action*" attribute. Supported actions are shown in the comments. If the action is "*None*", all the configurations and children of this table will be skipped.
- Configuration tables could contain more table specific attributes in case needed.

In this example, the *Action* is *None* for the *StdCfg* table. As such, SUM will skip updating the element *BoardMfgName* of the table *FRU*. On the other hand, SUM will try to update the value as *Enable* for the *HTTP* element of the *ServiceEnabling* table in the *OemCfg* table.

Notes:

- Child tables or configurable elements can be deleted to skip updates for these tables or configuration elements.
- Child tables or configurable elements cannot be without parents.
- The XML version line and the root table should not be deleted.
- For using tools to edit XML files, please refer to *Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files*.

4.7 RAID Configuration XML File format

The RAID configuration file displays editable RAID configuration elements in XML format for easier update. The example below shows how the RAID configurable elements are presented in this file.

- The XML version is shown in the first line.
- The root table name is "*RAIDCfg*". *<RAIDCfg>* and *</RAIDCfg>* are its tag pair. All information in the root table is enclosed between this tag pair.
- There could be three child tags for the root table: "*Information*" and "*RAIDController*" and *"Marvell9230RAIDController"*.
- "*Information*", "*RAIDController*" and *"Marvell9230RAIDController"* could have child tables.
- Configurable elements are listed in the "*Configuration*" field of each child table.
- Each configurable element has a tag pair. The element value is enclosed by its tag pair.
- Comments may be given following any element or table tag. Each comment is enclosed by the "*<!-*" and "*-->*" tags. The supported usage of each element and table are shown in the comments that follow.
- Configuration tables may have "*Action*" attributes. Supported actions are shown in the comments. If the action is "*None*", all configuration and child tables of this table will be skipped.
- Configuration tables may contain more table specific attributes when needed.

For Broadcom controller uses *"RAIDController"* table:

- To create a logical volume, the RAIDInfo action should be "*Change*" and the RAID action should be "*Create*". The "*PhysicalDriveList*" field must contain all drive IDs for RAID creation and the "ArrayID" field should be set to "-1".
- To delete a logical volume, the RAIDinfo action should be "*Change*", the RAID action should be "*Delete*" and assigned the corresponding logical drive ID or "*ALL*" to the "*DeletingLogicalDriveList*" field.
- To delete all arrays built in the RAID controller, the RAIDinfo action should be "*ClearAll*".
- To change RAID configuration, you have to delete the original RAID and create a new RAID with the "*Level*", "*Span*" and "*PhysicalDriveList*" fields properly modified.

- To enable the HDD LED in a RAID controller, add the drive ID to the "*LocatingPhysicalDriveIDList*" field and set the RAID action to "*Locate*".
- To disable the HDD LED in a RAID controller, add the drive ID to the "*UnlocatePhysicalDriveIDList*" field and set the RAID action to "*Unlocate*".

For Marvell controller uses "*Marvell9230RAIDController"* table:

- To create a logical drive, the RAIDInfo action should be "*Change*" and the RAID action should be "*Create*". The *"ArrayID"* field should be set to "0".
- To delete a logical drive, the RAIDinfo action should be "*Change*", the RAID action should be "*Delete*" and assigned the corresponding "LogicalDrive DriveID" to *"LogicalDriveDeleteID"*.
- To rebuild a logical drive, the RAIDinfo action should be "*Change*", the RAID action should be "*Rebuild*" and assigned the corresponding "LogicalDrive DriveID" to *"LogicalDriveRebuildID"*.
- To import a logical drive, the RAIDinfo action should be "*Change*", the RAID action should be "*Import*" and assigned the corresponding "LogicalDrive DriveID" to *"LogicalDriveImportID"*.

Notes:

- Child tables or configurable elements can be deleted to skip updating.
- Child tables or configurable elements must stick to the parent tables.
- The XML version line and the root table should not be deleted.
- Supported RAID levels on the Broadcom controller: 0/1/5/6/10/50/60
- Supported span values on the Broadcom controller:

RAID Level	Span Value	Minimum Number of Physical HDDs
0	1	1
1	1	2
5	1	3
6	1	3
10	2 or 4	4
50/60	3 or 4	6

- The number of physical hard drives must be a multiple of the "Span" value on the Broadcom controller.
- Marvell controller only supports RAID level 1.
- Marvell controller on AOC-SLG2-2TM2 supports up to two drives.
- For using tools to edit XML files, please refer to *Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files*.

Example:

```
<?xml version="1.0"?>
<RAIDCfg>
 <Information>
  <TotalRaidController>2</TotalRaidController>
 </Information>
 <RAIDController Action="Change" DeviceID="0">
  <!--Supported Action:None/Change-->
  <ControllerProperties Action="None">
   <!--Supported Action:None/Change-->
   <Configuration>
    <BiosBootMode>Stop on Error</BiosBootMode>
    <!--RAID controller BIOS boot mode, enumerated string value-->
    <!--Supported values: Stop on Error/Pause on Error/Ignore Errors/Safe Mode on Error-->
    <JbodMode>Disable</JbodMode>
    <!--RAID controller JBOD mode, enumerated string value-->
    <!--Supported values: Enable/Disable-->
   </Configuration>
  </ControllerProperties>
  <RAIDInfo Action="Change">
   <!--Supported Action:None/Change/ClearAll-->
   <RAID Action="None" ArrayID="-1">
    <!--Supported Action:None/Add/Delete/Create/Locate/Unlocate-->
    <Information>
     <PhysicalDriveCount>0</PhysicalDriveCount>
     <!--Total number of physical drives in this RAID-->
     <LogicalDriveCount>0</LogicalDriveCount>
     <!--Total number of logical drives in this RAID-->
     <LocatedPhysicalDriveList></LocatedPhysicalDriveList>
     <!--located physical drives-->
     <FreeSize>0</FreeSize>
     <!--Free size of RAID, unit: MB-->
     <LogicalDriveInfo></LogicalDriveInfo>
```

```
</Information>
<Configuration>
 <!--For each field, default support Create/Add actions if not specially commented-->
 <Level>RAID0</Level>
 <!--RAID level, enumerated string value-->
 <!--Supported values: RAID0/RAID1/RAID5/RAID6/RAID10/RAID50/RAID60-->
 <!--Only used for "Create" action-->
 <Span>1</Span>
 <!--PD span value, integer value-->
 <!--For RAID 0/1/5/6, valid value is 1-->
 <!--For RAID 10, valid value is 2 or 4-->
 <!--For RAID 50/60, valid value is 3 or 4-->
 <!--Only used for "Create" action-->
 <PhysicalDriveList></PhysicalDriveList>
 <!--Number of physical hard drive must be multiple of "Span" value-->
 <!--Physical drive ID list of this RAID, integer values separated by comma.-->
 <!--Can not use physical hard drive which present in other RAID.-->
 <!--Can not use "Error" status physical HDD.-->
 <!--Can not use repeated physical hard drive ID in same RAID.-->
 <!--Physical hard drive ID can not use negative number.-->
 <!--Physical hard drive count can't be more than 32.-->
 <!--For RAID0, minimum number of physical HDD is 1.-->
 <!--For RAID1, minimum number of physical HDD is 2.-->
 <!--For RAID5, minimum number of physical HDD is 3.-->
 <!--For RAID6, minimum number of physical HDD is 3.-->
 <!--For RAID10, minimum number of physical HDD is 4.-->
 <!--For RAID50, minimum number of physical HDD is 6.-->
 <!--For RAID60, minimum number of physical HDD is 6.-->
 <!--Only used for "Create" action.-->
 <NewLogicalCount>1</NewLogicalCount>
 <!--Number of new Logical drive to be created/added-->
 <!--Integer value, valid value from 1 to 16-->
```

<!--Can not run "Add" action when RAID has no any physical hard drive.-->

<!--Only used for "Create" and "Add" action-->

<PercentageToUsed>100</PercentageToUsed>

<!--Percentage to use, integer value between 1 and 100.-->

<!--Only used for "Create" and "Add" action-->

<StripSize>256KB</StripSize>

<!--Strip size of each logical drive-->

<!--Enumerated integer value, unit is Byte-->

<!--Valid value: 64KB/128KB/256KB/512KB/1MB-->

<!--Default value: 256KB-->

<!--Only used for "Create" and "Add" action-->

<LogicalDriveName></LogicalDriveName>

<!--Name of logical drive, string value-->

<!--Maximum length: 15, empty string is accepted-->

<!--Only used for "Create" and "Add" action-->

<LogicalDriveReadPolicy>No Read Ahead</LogicalDriveReadPolicy>

<!--Read policy of logical drive, enumerated string value-->

<!--Possible values: No Read Ahead/Always Read Ahead-->

<!--Default value: No Read Ahead-->

<!--The value in this field does not indicate current setting, it is the reference value for configuring purpose only-->

<!--Only used for "Create" and "Add" action-->

<LogicalDriveWritePolicy>Write Back</LogicalDriveWritePolicy>

<!--Write policy of logical drive, enumerated string value-->

<!--Possible values: Write Through/Write Back/Write Back With BBU-->

<!--Default value: Write Back-->

<!--The value in this field does not indicate current setting, it is the reference value for configuring purpose only-->

<!--Only used for "Create" and "Add" action-->

<LogicalDriveIoPolicy>Direct IO</LogicalDriveIoPolicy>

<!--IO policy of logical drive, enumerated string value-->

<!--Possible values: Direct IO/Cached IO-->

<!--Default value: Direct IO-->

<!--The value in this field does not indicate current setting, it is the reference value for configuring purpose only-->

<!--Only used for "Create" and "Add" action-->

<AccessPolicy>Read Write</AccessPolicy>

<!--Access policy of logical drive, enumerated string value-->

<!--Possible values: Read Write/Read Only/Blocked-->

<!--Default value: Read Write-->

<!--The value in this field does not indicate current setting, it is the reference value for configuring purpose only-->

<!--Only used for "Create" and "Add" action-->

<DiskCachePolicy>UnChanged</DiskCachePolicy>

<!--Cache policy of logical drive, enumerated string value-->

<!--Possible values: UnChanged/Enable/Disable-->

<!--Default value: UnChanged-->

<!--The value in this field does not indicate current setting, it is the reference value for configuring purpose only-->

<!--Only used for "Create" and "Add" action-->

<InitState>No Init</InitState>

<!--Initial state of logical drive, enumerated string value-->

<!--Possible values: No Init/Quick Init/Full Init-->

<!--Default value: No Init-->

<!--The value in this field does not indicate current setting, it is the reference value for configuring purpose only-->

<!--Only used for "Create" and "Add" action-->

<DeletingLogicalDriveList></DeletingLogicalDriveList>

<!--Logical drive ID list for deleting, integer values separated by comma-->

<!--Logical drive for deleting can not use negative number-->

<!--Logical drive for deleting should be physical hard drive of this RAID-->

<!--Can not use repeated physical hard drive ID in same RAID.-->

<!--All logical physical hard drives of RAID will be deleted when fill "ALL"-->

<!--Can not run "Delete" action when RAID has no any physical hard drive.-->

<!--Only used for "Delete" action.-->

<LocatingPhysicalDriveIDList></LocatingPhysicalDriveIDList>

<!--Physical drive ID list for locating: integer values separated by comma-->

```
      <!--Physical drive for locating can not use negative number-->
      <!--Physical drive for locating should be physical hard drive of this RAID-->
      <!--All physical hard drives of RAID will be located when fill "ALL"-->
      <!--Can not use repeated physical hard drive ID in same RAID.-->
      <!--Can not run "Locate" action when RAID has no any physical hard drive.-->
      <!--Only used for "Locate" action-->
      <UnlocatePhysicalDriveIDList></UnlocatePhysicalDriveIDList>
      <!--Physical drive ID list for unlocating: integer values separated by comma-->
      <!--Physical drive for unlocating can not use negative number-->
      <!--Physical drive for unlocating should be physical hard drive of this RAID-->
      <!--All physical hard drives of RAID will be unlocated when fill "ALL"-->
      <!--Can not use repeated physical hard drive ID in same RAID.-->
      <!--Can not run "Unlocate" action when RAID has no any physical hard drive.-->
      <!--Only used for "Unlocate" action-->
    </Configuration>
   </RAID>
  </RAIDInfo>
</RAIDController>
<Marvell9230RAIDController Action="Change" DeviceID="0">
  <!--Supported Action:None/Change-->
  <ControllerProperties>
   <Information>
    <Controller>Marvell</Controller>
    <!--RAID controller-->
    <ControllerName>MRVL Storage System</ControllerName>
    <!--RAID controller name-->
    <ControllerSpeed>5.0 GT/s</ControllerSpeed>
    <!--RAID controller speed-->
    <ControllerStatus>OK</ControllerStatus>
    <!--RAID controller status-->
    <ChipRevision>a1</ChipRevision>
    <!--RAID controller chip revision-->
```

```
    <ControllerPCIELinkWidth>2x Width</ControllerPCIELinkWidth>
    <!--RAID controller PCIE link width-->
    <RomVersion>0.0.21.1005</RomVersion>
    <!--RAID controller rom version-->
    <LoaderVersion>2.1.0.1009</LoaderVersion>
    <!--RAID controller loader version-->
    <LegacyBIOSVersion>1.0.0.1031</LegacyBIOSVersion>
    <!--RAID controller legacy BIOS version-->
    <UEFIAHCIDriverVersion>1.1.21.1002</UEFIAHCIDriverVersion>
    <!--RAID controller UEFI AHCI driver version-->
    <I2CProtocolVersion>0.0.0.20</I2CProtocolVersion>
    <!--RAID controller I2C protocol version-->
    <PN></PN>
    <!--RAID controller PN-->
    <AOCVersion></AOCVersion>
    <!--RAID controller AOC version-->
    <SerialNumber></SerialNumber>
    <!--RAID controller serial number-->
    <FirmwareVersion></FirmwareVersion>
    <!--RAID controller firmware version-->
    <Batch></Batch>
    <!--RAID controller batch-->
  </Information>
</ControllerProperties>
<PhysicalDriveInfo>
  <Information>
    <!--Physical hard drive information, this region is read only.-->
    <DriveCount>2</DriveCount>
    <PhysicalDrive DriveID="0">
      <EnclosureID>0</EnclosureID>
      <!--Enclosure ID, string value-->
      <DriveStatus>OK</DriveStatus>
```

```
  <!--Physical drive alive status, enumerated string value-->
  <!--Possible values: OK/Warning-->
  <Temperature>46</Temperature>
  <!--Physical drive temperature in degree C, integer value-->
  <Capacity>480</Capacity>
  <!--Physical drive capacity in Gigabyte, integer value-->
  <ModelName>Micron_5300_MTFDDAV480TDS</ModelName>
  <!--Physical drive model name, string value-->
  <Revision> D3MU001</Revision>
  <!--Physical drive firmware revision, string value-->
  <SerialNumber>ABCDE</SerialNumber>
  <!--Physical drive serial number, string value-->
  <LinkSpeed>6</LinkSpeed>
  <!--Physical drive link speed value, string values-->
  <!--Unit is Gb/s-->
  <FirmwareConfiguredState>OK</FirmwareConfiguredState>
  <!--Firmware status of physical drive.-->
  <PredictedFail>false</PredictedFail>
  <!--Physical drive predicted fail-->
  <!--Possible values: true/false-->
 </PhysicalDrive>
 <PhysicalDrive DriveID="1">
  <EnclosureID>1</EnclosureID>
  <!--Enclosure ID, string value-->
  <DriveStatus>OK</DriveStatus>
  <!--Physical drive alive status, enumerated string value-->
  <!--Possible values: OK/Warning-->
  <Temperature>47</Temperature>
  <!--Physical drive temperature in degree C, integer value-->
  <Capacity>480</Capacity>
  <!--Physical drive capacity in Gigabyte, integer value-->
  <ModelName>Micron_5300_MTFDDAV480TDS</ModelName>
```

```
    <!--Physical drive model name, string value-->
    <Revision> D3MU001</Revision>
    <!--Physical drive firmware revision, string value-->
    <SerialNumber>ABCDE</SerialNumber>
    <!--Physical drive serial number, string value-->
    <LinkSpeed>6</LinkSpeed>
    <!--Physical drive link speed value, string values-->
    <!--Unit is Gb/s-->
    <FirmwareConfiguredState>OK</FirmwareConfiguredState>
    <!--Firmware status of physical drive.-->
    <PredictedFail>false</PredictedFail>
    <!--Physical drive predicted fail-->
    <!--Possible values: true/false-->
   </PhysicalDrive>
  </Information>
</PhysicalDriveInfo>
<RAIDInfo Action="Change">
  <!--Supported Action:None/Change-->
  <RAID Action="None" ArrayID="0">
   <!--Supported Action:None/Delete/Create/Rebuild/Import-->
   <Information>
    <PhysicalDriveCount>2</PhysicalDriveCount>
    <!--Total number of physical drives in this RAID-->
    <LogicalDriveCount>1</LogicalDriveCount>
    <!--Total number of logical drives in this RAID-->
    <LogicalDrive DriveID="0">
     <DriveStatus>OK</DriveStatus>
     <!--Logical drive alive status-->
     <!--Possible values: OK/Warning-->
     <Capacity>447</Capacity>
     <!--Logical drive capacity, integer value-->
     <!--Unit is GB-->
```

<RaidLevelQualifier>RAID1</RaidLevelQualifier>
<!--RAID level qualifier of logical drive, enumerated value-->
<!--Possible values: RAID1-->
<LDStripSize>64K</LDStripSize>
<!--Strip size of logical drive, enumerated value-->
<!--Unit is Byte-->
<!--Possible values: 32K/64K-->
<PD0Registered>Yes</PD0Registered>
<!--Physical drive #0 registered-->
<!--Possible values: Yes/No-->
<PD1Registered>Yes</PD1Registered>
<!--Physical drive #1 registered-->
<!--Possible values: Yes/No-->
<FirmwareState>Optimal</FirmwareState>
<!--Firmware state for this RAID, enumerated string value-->
<!--Possible values: Offline/Foreign/Degraded/Rebuilding/Optimal-->
<Name>SuperFuck</Name>
<!--Name of logical drive, string value-->
</LogicalDrive>
</Information>
<Configuration>
<!--For each field, default support Create actions if not specially commented-->
<Level>RAID1</Level>
<!--RAID level, enumerated string value-->
<!--Only supported value: RAID1-->
<!--Only used for "Create" action-->
<StripSize>32K</StripSize>
<!--Strip size of each logical drive-->
<!--Enumerated integer value, unit is Byte-->
<!--Valid value: 32K/64K-->
<!--Default value: 64K-->
<!--Only used for "Create" action-->

```
        <LogicalDriveName><![CDATA[]]></LogicalDriveName>
        <!--Name of logical drive, string value-->
        <!--Maximum length: 15-->
        <!--Should not contains space and double quote-->
        <!--Only used for "Create" action-->
        <LogicalDriveDeleteID>0</LogicalDriveDeleteID>
        <!--Delete virtual drive ID, integer value-->
        <!--ID number should be LogicalDrive DriveID-->
        <!--Should not set bigger than LogicalDrive DriveID-->
        <!--Only used for "Delete" action-->
        <LogicalDriveImportID>0</LogicalDriveImportID>
        <!--Import virtual drive ID, integer value-->
        <!--ID number should be LogicalDrive DriveID-->
        <!--Should not set bigger than LogicalDrive DriveID-->
        <!--Only used for "Import" action-->
        <LogicalDriveRebuildID>0</LogicalDriveRebuildID>
        <!--Rebuild virtual drive ID, integer value-->
        <!--ID number should be LogicalDrive DriveID-->
        <!--Should not set bigger than LogicalDrive DriveID-->
        <!--Only used for "Rebuild" action-->
      </Configuration>
    </RAID>
  </RAIDInfo>
 </Marvell9230RAIDController>
</RAIDCfg>
```

For Broadcom controller:

- To create an array:

  Create a RAID 10 array with Span 2 and 4 HDDs and "*ArrayID*" field can be set to "-1":

For array ID, “-1” will be used when no array exists. This setting enables a dummy array table for you to create the first array. Note that for the creation action, “*ArrayID*” is meaningless and array ID will be generated after the array is created.

```
<RAIDInfo Action="Change">
        <RAID Action="Create" ArrayID="-1">
            <Level>RAID10</Level>
            <Span>2</Span>
            <PhysicalDriveList>0,1,2,3</PhysicalDriveList>To create two or more arrays:
<RAIDInfo Action="Change">
```

Array 1

```
        <RAID Action="Create" ArrayID="-1">
            <Level>RAID10</Level>
            <Span>2</Span>
            <PhysicalDriveList>0,1,2,3</PhysicalDriveList>
```

Array 2

```
        <RAID Action="Create" ArrayID="-1">
            <Level>RAID10</Level>
            <Span>2</Span>
            <PhysicalDriveList>4,5,6,7</PhysicalDriveList>
```

- To delete logical drives:

  Delete logical drive 0 and 1 from “Array0”.

```
<RAIDInfo Action="Change">
        <RAID Action="Delete" ArrayID="0">
            <DeletingLogicalDriveList>0,1</DeletingLogicalDriveList>
```

- To delete an array:

  Use “ALL” to delete every logical drive from “Array0”. After this, “Array0” will be:

```
<RAIDInfo Action="Change">
        <RAID Action="Delete" ArrayID="0">
            <DeletingLogicalDriveList>ALL</DeletingLogicalDriveList>
```

- To delete all arrays:

  Use “*ClearAll*” to delete every array. After this, every array will disappear.

```
<RAIDInfo Action="ClearAll">
```

- Locate HDDs:

  Locate HDD1/HDD2/HDD3 in “Array0”. LEDs of HDD1/HDD2/HDD3 will be lighted.

```
<RAIDInfo Action="Change">
        <RAID Action="Locate" ArrayID="0">
                <LocatingPhysicalDriveIDList>1,2,3</LocatingPhysicalDriveIDList>
```

- Unlocate HDDs:

  Unlocate HDD1/HDD4 in “Array0”. LEDe of HDD1/HDD4 will be dimmed.

```
<RAIDInfo Action="Change">
        <RAID Action="Unlocate" ArrayID="0">
                <UnlocatePhysicalDriveIDList>1,4</UnlocatePhysicalDriveIDList>
```

For Marvell controller:

- To create a logical drive:

```
<RAIDInfo Action="Change">
        <RAID Action="Create" ArrayID="0">
                <Configuration>
                        <Level>RAID1</Level>
                        <StripSize>32K</StripSize>
                        <LogicalDriveName><![CDATA[dummy]]></LogicalDriveName>
```

- To delete a logical drive:

  Delete logical drive 0.

```
<RAIDInfo Action="Change">
        <RAID Action="Delete" ArrayID="0">
                <Configuration>
                        <LogicalDriveDeleteID>0</LogicalDriveDeleteID>
```

- To import a logical drive:

  Import logical drive 0.

```
<RAIDInfo Action="Change">
        <RAID Action="Import" ArrayID="0">
```

```
<Configuration>
    <LogicalDriveImportID>0</LogicalDriveImportID>
```

- To rebuild a logical drive:

  Rebuild logical drive 0.

```
<RAIDInfo Action="Change">
    <RAID Action="Rebuild" ArrayID="0">
        <Configuration>
            <LogicalDriveRebuildID>0</LogicalDriveRebuildID>
```

- **Note:** A system needs to reboot after importing logical drives for the changes to take effect.

4.8 CMM Configuration XML File Format

The CMM configuration file contains CMM configuration elements in XML format for an easier update process. An example below shows how this file demonstrates the CMM configurable elements.

```
<?xml version="1.0"?>
<CmmCfg>
  <!--You can remove unnecessary elements so that-->
  <!--their values will not be changed after update-->
  <StdCfg Action="None">
    <!--Supported Action:None/Change-->
    <!--Standard Cmm configuration tables-->
    <SOL Action="Change">
      <!--Supported Action:None/Change-->
      <Configuration>
        <!--Configuration for SOL properties-->
        <Access>Enable</Access>
        <!--Enable/Disable-->
      </Configuration>
    </SOL>
  </StdCfg>
  <OemCfg Action="Change">
      <!--Supported Action:None/Change-->
      <!--OEM Cmm configuration tables-->
      <ServiceEnabling Action="Change">
        <!--Supported Action:None/Change-->
        <Configuration>
          <!--Configuration for ServiceEnabling-->
          <HTTP>Enable</HTTP>
          <!--Enable/Disable-->
        </Configuration>
      </ServiceEnabling>
  </OemCfg>
</CmmCfg>
```

- The version of the xml file is shown in the first line.
- The root table name is "*CmmCfg*". Its name tag pairs are *<CmmCfg>* and *</CmmCfg>*. All information of the root table is enclosed in this name tag pair.
- "*StdCfg*" and "*OemCfg*" could be two child tables for the root table.
- "*StdCfg*" and "*OemCfg*" could have child tables.
- Configurable elements are listed in the "*Configuration*" field in each child table.
- Each configurable element has a name tag pair. The element value is enclosed in its name tag pair.
- Comments could be given following any element or table name tag. Each comment is enclosed in the tags "*<!--*" and "*-->*". The use of each element and table is shown in its following comments.
- Configuration tables could have "*Action*" attribute. Supported actions are shown in the comments. If action is "*None*", all the configurations and children of this table will be skipped.
- Configuration tables could contain more specific table attributes in case they are needed.

In this example, the *Action* is *None* for the *StdCfg* table. As such, SUM will skip updating the element *Access* of the table *SOL*. On the other hand, SUM will try to update the value as *Enable* for the *HTTP* element of the *ServiceEnabling* table in the *OemCfg* table.

Notes:

- Child tables or configurable elements can be deleted to skip updates for these tables or configuration elements.
- Child tables or configurable elements cannot be without parents.
- The XML version line and the root table should not be deleted.
- For using tools to edit XML files, please refer to *Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files*.

4.9 TUI

SUM 2.2.0 or later supports the text-based user interface (TUI) to make the edits of the settings more user-friendly, providing nice visibility, intuitive and lower learning curve. System configurations can be easily rendered with TUI like BIOS configurations. It supports the operating systems Linux, Windows and FreeBSD. Some of the features are:

- **Easy Operation**

With the visual menu, information display is more intuitive than an XML file. A user can make changes without learning rules. For example, when a function is disabled, all the dependent settings become invalid or meaningless. TUI will then hide the settings accordingly.

- **Real-Time Feedback**

SUM with TUI allows a user to check input format settings in real time and get feedback immediately. For example, when a data constraint violation occurs, an error message pops up in TUI. The user can find out about errors without waiting for the execution to be completed.

- **GUI-Free Environment**

In practice, GUI packages are usually not installed on most Unix-like servers. TUI provides an interactive interface on text-based system without GUI packages.

- **Automatic Configuration of Terminal Settings**

Terminal settings are automatically configured to ensure display quality.

4.9.1 TUI General Reminders

Note the following information before using TUI.

- The TUI feature is not supported by any terminal multiplexer.
- Do not resize the terminal display while executing a command with the --TUI option.
- For optimized display, SUM automatically configures your terminal settings. Refer to the table below to see if the related environment variables are changed accordingly.

Operating System	Environment Variables	Variable Values
Windows	code page	437 (US English)
Linux	TERM	linux
FreeBSD	TERM	linux

- After you finish using TUI, your original terminal settings will be automatically restored. If restoration fails, locate and run the shell script "restore_terminal_config.sh" under the current working directory. The execution command as below:

  Linux and FreeBSD:

  ```
  [shell]# source restore_terminal_config.sh
  ```

  Windows:

  ```
  X:\working directory> restore_terminal_config.bat
  ```

- On Windows, please adjust font size by yourself if the font size is too small to operate.
- TUI does not support mouse operation.
- On FreeBSD, when running on local terminal with vt driver (default driver after FreeBSD 11), SUM changes the font to tui.fnt when entering TUI, and changes the font to **default font** when exiting TUI. You can rename or remove the file ExternalData/tui.fnt to disable this behavior.
- External/tui.fnt is converted from terminus-u12n.bdf by vtfontcvt, check *Appendix D* for the license.

4.9.2 BIOS TUI Configuration

TUI Display

SUM with TUI simulates a BIOS setup design and its display dimension is set to 30 rows by 100 columns. If SUM fails to resize the terminal with the current terminal settings, it will try to change font type and font size for optimized display. The commands to change terminal dimensions on different operating systems are listed in the table below.

4.9.2.1

Operating System	OS Command to Change Terminal Dimensions
Windows	mode con lines=30 cols=100
Linux	stty cols 100 rows 30
FreeBSD	(sc driver) Local host: Change console video mode by vidcontrol command (vt driver) Local host: Change console font by vidcontrol -f command. Remote console: stty cols 100 rows 30

Terminal dimensions are automatically changed so that some settings are changed as well.

Notes:

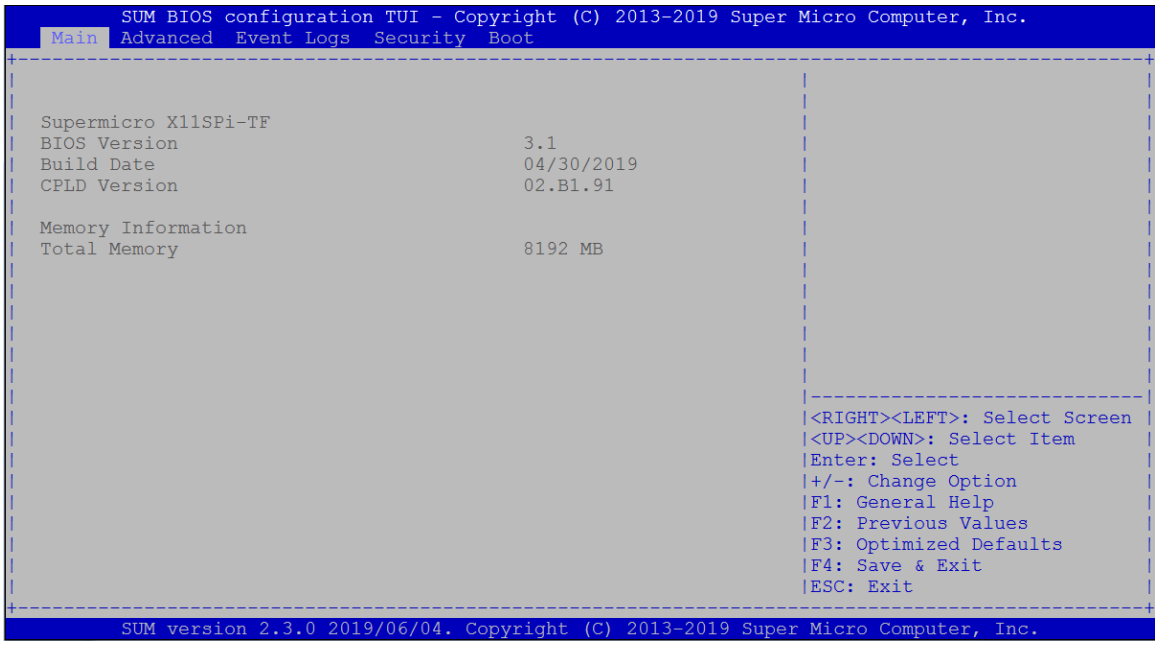
- The command "GetCurrentBiosCfg" is supported. For details on running the command GetCurrentBiosCfg, please refer to *5.3.3 Receiving Current BIOS Settings*.
- Some settings and requirements may vary on different BIOS systems where TUI is run.

How to Use

- **Using Arrow Keys**

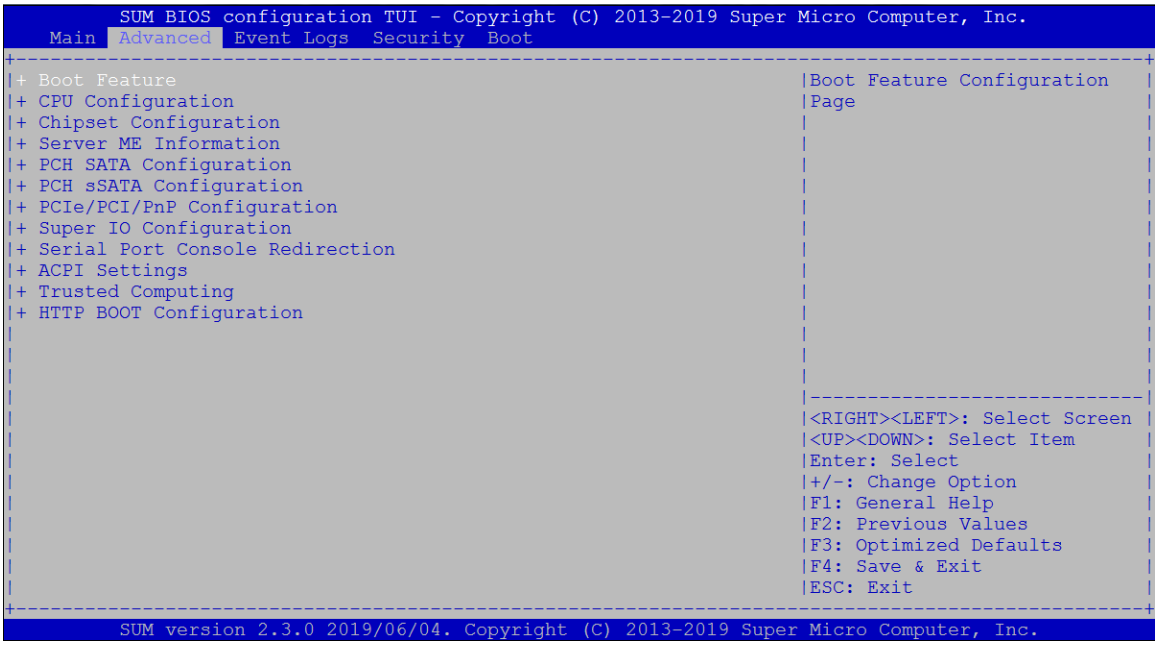
When you first enter the SUM BIOS Setup Utility, the “Main” root menu setup appears on screen. Press the arrow keys **<RIGHT>** and **<LEFT>** to navigate between menu tabs.

4.9.2.2



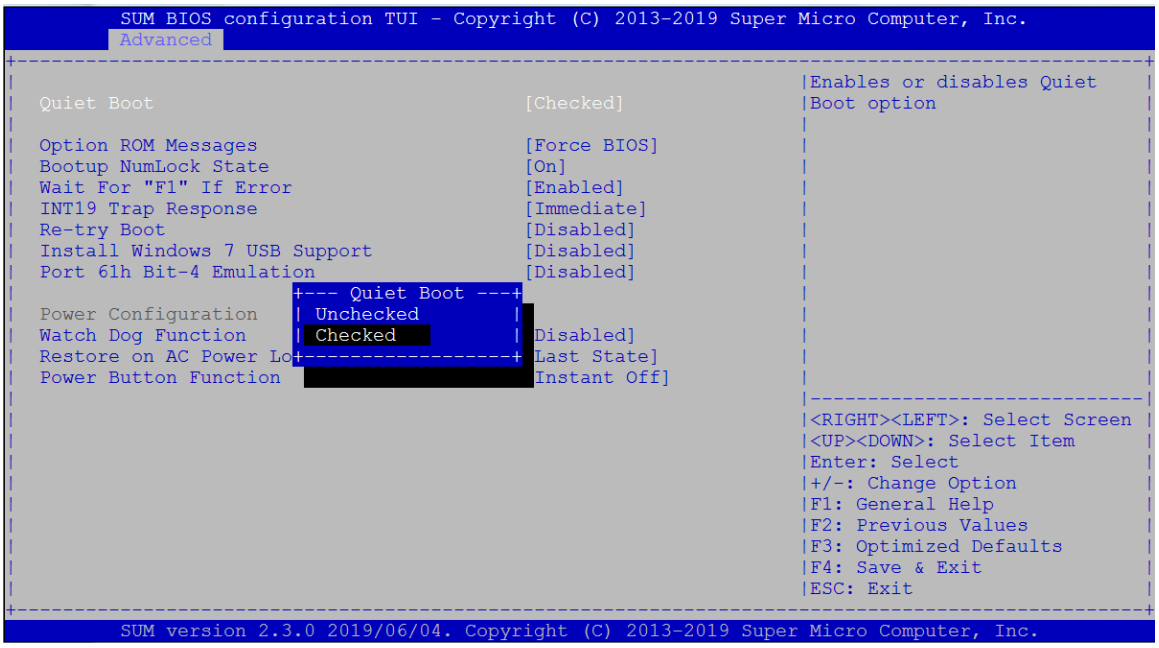
- **Setting Values**

A “+” symbol before an option on a menu indicates that a sub-menu can be expanded for further configuration. To change a setting value, you can press the keys **<+>** and **<->**. Or you can press the **<Enter>** key to call up a dialog box for configuration.



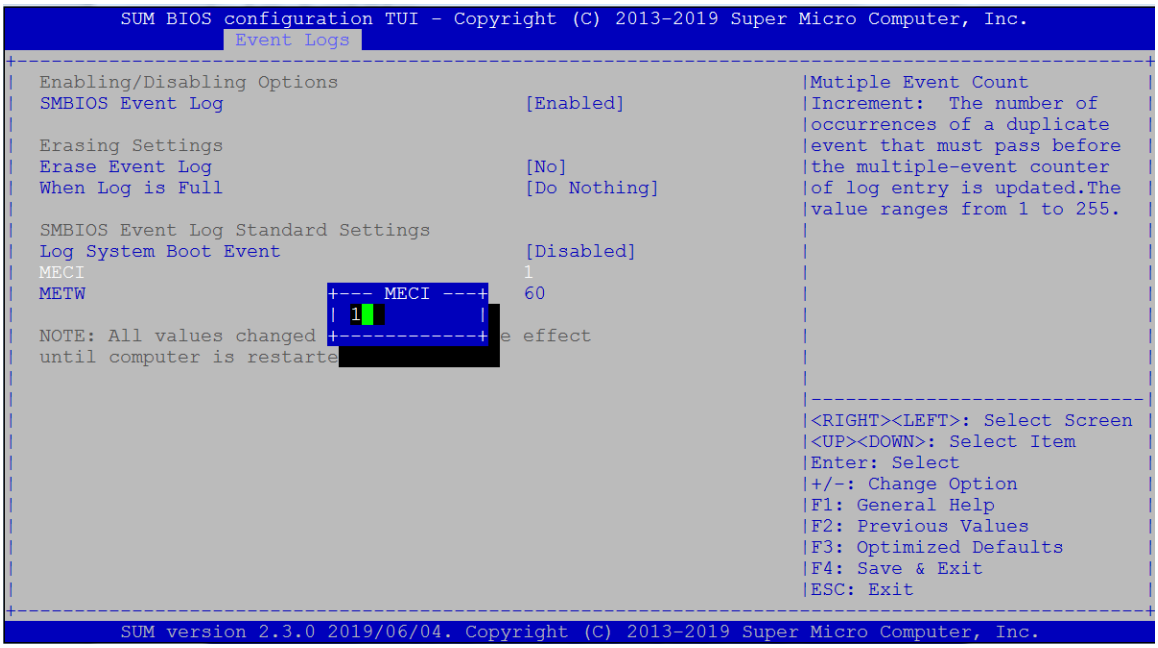
- **Using a Check Box to Enable/Disable a Function**

Some functions are allowed to be enabled or disabled. To change the setting, press the **<Enter>** key to call up a dialog box. Press the **<UP>** and **<DOWN>** arrow keys to make a selection. To disable a function, select **Unchecked**. To enable a function, select **Checked**.



- **Setting Numeric Values**

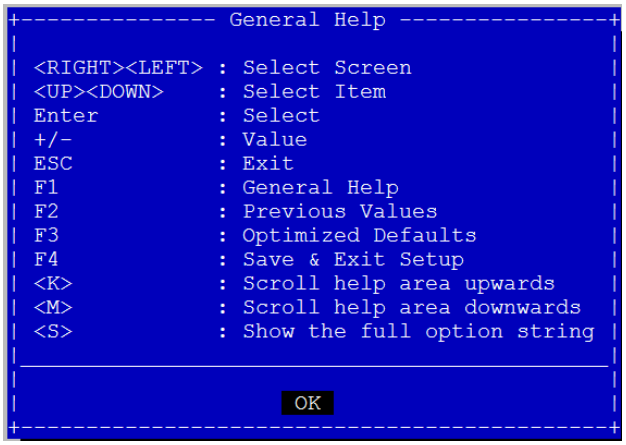
A value may be limited due to the BIOS. You can press the number keys to enter the desired value, or press the keys **<+>** and **<->** to adjust your value within the range. If an input value is incorrect, a warning message appears on screen.



Getting General Help

For general help information, press the **<F1>** key. A message box appears.

4.9.2.3

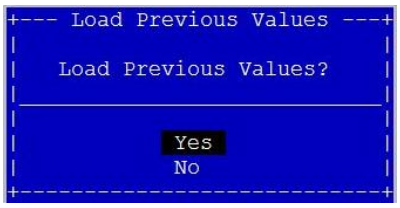


4.9.2.4

Loading Previous Values

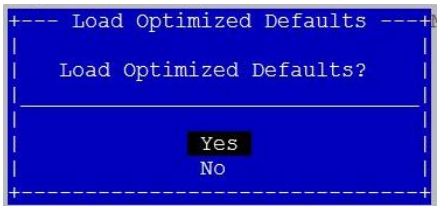
To load the previous values to all configurations, press the **<F2>** key. A message appears for confirmation.

4.9.2.5



Loading Optimized Values

To return all configurations to the default values, press the **<F3>** key. A message appears for confirmation.

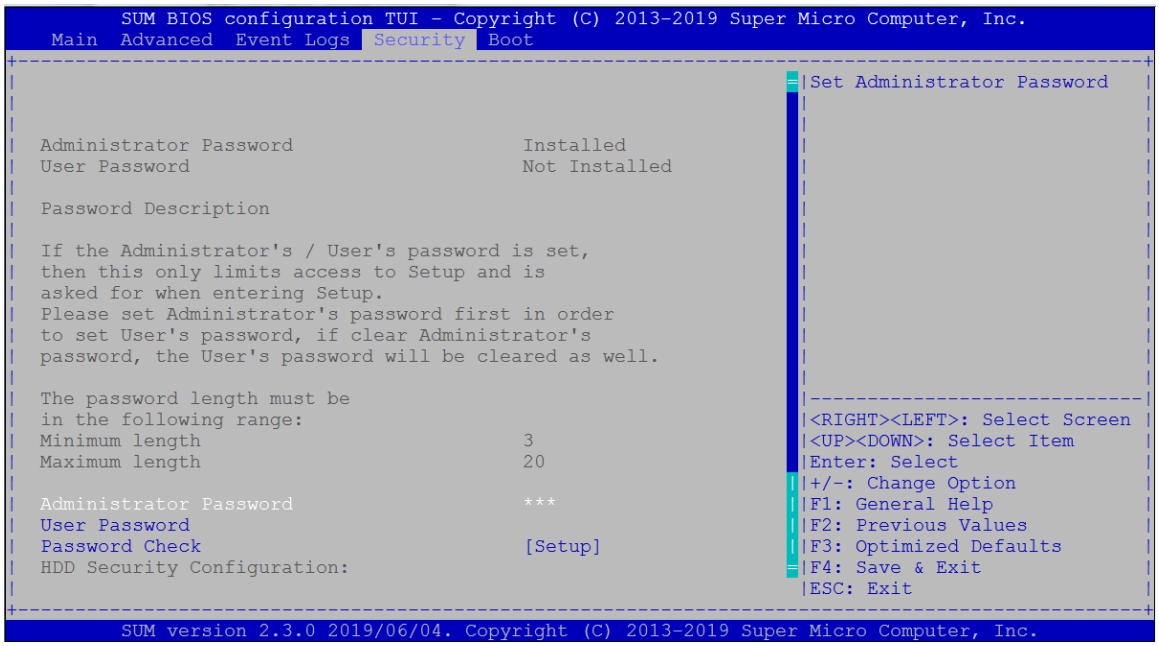


Setting a Password

Go to **Security**, select **Administrator Password** and press the **<Enter>** key to set a password. Note the following when you set a password:

4.9.2.6

- If you have already set passwords in your BIOS, a series of three asterisks on the Security page indicates that a password is created (see the figure below).
- The password length may vary depending on the BIOS you use. For example, the length of the password can be from 3 to 20 characters long (see the figure below).

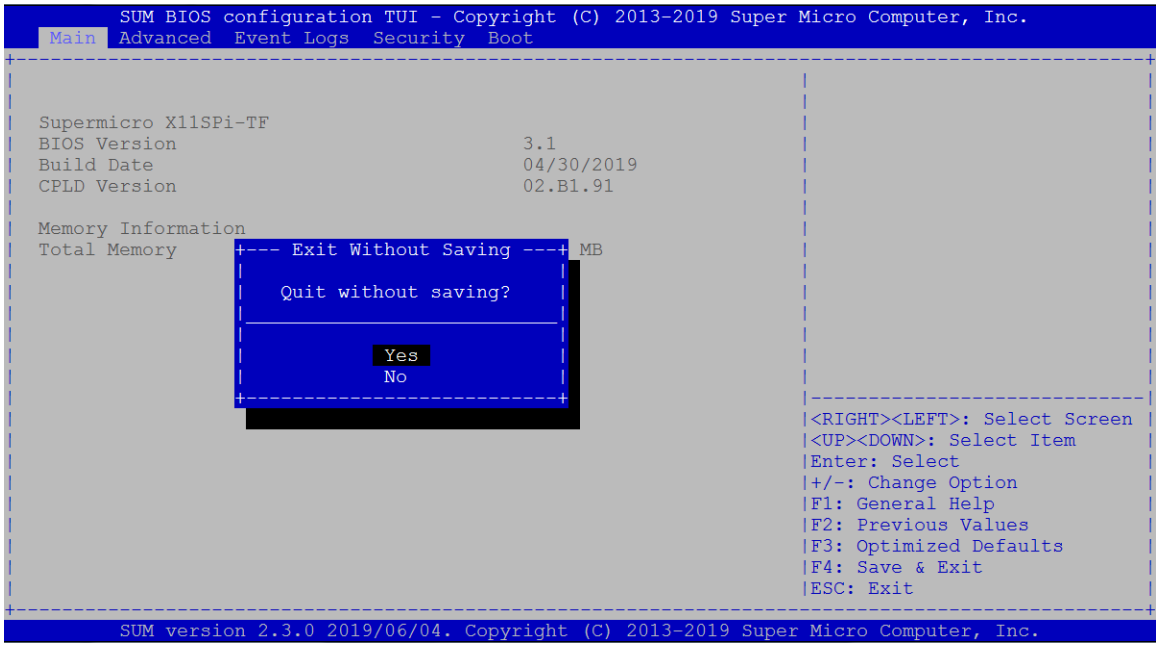


Exiting the TUI

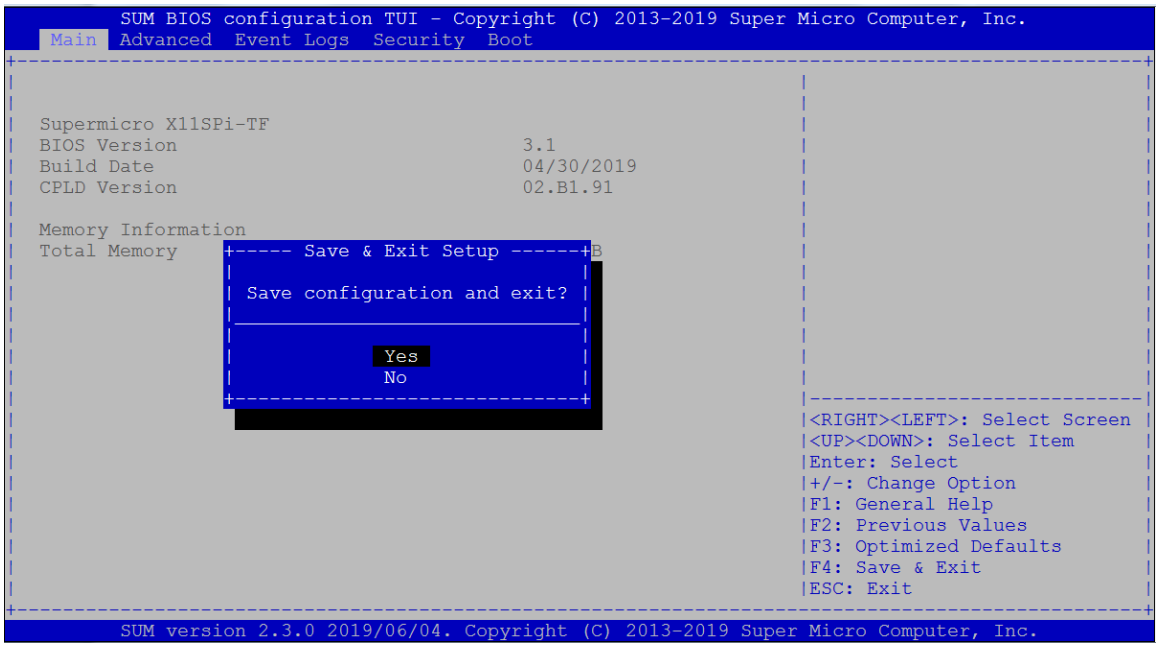
Two methods are available to exit the SUM BIOS configuration TUI.

- To exit the TUI without saving any configurations, press the **<ESC>** key. A message appears on the screen for confirmation. Note that this only works on the root menu. You will be returned to the previous menu when you press the **<ESC>** key in submenus.

4.9.2.7



- To save the configurations and exit the TUI, press the **<F4>** key. A message appears on the screen for confirmation.



4.10 Redfish Host Interface

Redfish Host Interface can be used by software running on a computer system to access the Redfish Service used to manage the computer system. For details on Redfish Host Interface, refer to the Redfish Host Interface Specification by DMTF.

Since SUM 2.5.0, some commands support Redfish Host Interface on X12/H12 and later platforms except the H12 non-RoT system.

4.10.1 Using Redfish Host Interface

Syntax:

```
sum -I Redfish_HI -u <username> -p <password> -c <command>
```

Unlike normal in-band operation, the <username> and <password> are needed to access the managed system.

4.10.2 Supported Commands

Currently, the following commands support Redfish Host Interface for in-band usage: UpdateBios, UpdateBmc, ActivateProductKey, QueryProductKey, BiosRotManage, BmcRotManage, UpdateRaidController ,GetRaidControllerInfo, GetCpldInfo, UpdateCpld, GetPMemInfo and UpdatePMem.

Example:

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateBios --file
SMCI_BIOS.rom

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateBmc --file
SMCI_BMC.rom

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c ActivateProductKey --key
1111-1111-1111-1111-1111-1111

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c QueryProductKey
```

5 Managing a Single System

In this chapter, we describe basic user operations for managing a single system, either through the OOB channel or, if applicable, through the in-band channel. In-band channel usage is similar to OOB usage except for several differences:

1. For in-band usage, do not use the -l, -i, -u, -p and -f options.
2. For in-band usage, supported commands and their node product key requirement might be different (see *Appendix B. Management Interface and License Requirements*).
3. A Linux driver might be required for in-band usage. For details, please see *2.3 Setting Up In-Band Managed Systems*. If a Linux driver is required and you are executing SUM in this server for the first time, you have to copy and paste the OS specific driver file "sum_bios.ko" under the SUM_HOME/driver directory to the SUM_HOME directory. For example, if the OS is RHEL 5.x. execute

```
[SUM_HOME]# cp ./driver/RHL5_x86_64/sum_bios.ko ./
```

5.1 Key Management for a Single System

5.1.1 Activating a Single Managed System

To activate systems individually, follow these steps by using the command “ActivateProductKey”.

1. Obtain a node product key from Supermicro. See *3.1 Receiving Product Keys from Supermicro*.
2. Use the following SUM command.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
ActivateProductKey [--key <nodeproductkey> | --key_file <file name>]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ActivateProductKey --
key 1111-1111-1111-1111-1111-1111

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ActivateProductKey --key
'{"ProductKey":{"Node":{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111112222222222222223333333333333ab
abababababababababababbabcdcdcdcdcdcdcdccdcdcddcdefefefefefefefefeefefefefghghghghghghghghghgh"}}'

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ActivateProductKey --
key_file mymacs.txt.key
```

In-Band:

```
[SUM_HOME]# ./sum -c ActivateProductKey --key 1111-1111-1111-1111-1111-1111

[SUM_HOME]# ./sum -c ActivateProductKey --key
'{"ProductKey":{"Node":{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111112222222222222223333333333333ab
abababababababababababbabcdcdcdcdcdcdcdccdcdcddcdefefefefefefefefeefefefefghghghghghghghghghgh"}}'

[SUM_HOME]# ./sum -c ActivateProductKey --key_file mymacs.txt.key
```

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c ActivateProductKey --key
1111-1111-1111-1111-1111-1111

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c ActivateProductKey --
key_file mymacs.txt.key
```

Notes:

- A node product key in JSON format must be put in single quotation marks.
- When activating a key in JSON format in Windows, the JSON key string cannot contain any spaces.
- For details on the format of a product key file (mymacs.txt.key)., see *3.1 Receiving Product Keys from Supermicro.*

5.1.2 Querying the Node Product Keys

To query the node product keys activated in the managed system, use the command "QueryProductKey."

Syntax:

```
sum [[-i <IP or host name> | -I <Redfish_HI>] -u <username> -p <password>] -c
QueryProductKey
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c QueryProductKey
```

In-Band:

```
[SUM_HOME]# ./sum -c QueryProductKey

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c QueryProductKey
```

The console output contains the information below. Each line is a node product key that has been activated in the managed system. In each line, the first field is the key name. All keys have extra fields describing the detailed attributes if available.

```
SFT-OOB-LIC
SFT-DCMS-SINGLE ,    invoice: X8800693687A,      creation date: 2019/12/03
SFT-SPM-LIC     ,    invoice: X8800693688A,      creation date: 2019/12/04
SFT-DCMS-SVC-KEY,    invoice: X8800693689A,      creation date: 2019/12/04
Number of product keys: 4
```

5.2 System Checks for a Single System

5.2.1 Checking OOB Support

Use the command "CheckOOBSupport" to check if both BIOS and BMC firmware images support OOB functions.

Notes:

- If your BMC does not support OOB functions, you can update the BMC firmware image using the SUM "UpdateBmc" command.
- To update the BIOS in the managed system to support OOB functions, you can use the SUM "UpdateBios" command (either in-band or OOB) to flash BIOS even when BIOS does not support OOB functions. For details, see *5.3.2 Updating the BIOS Firmware Image*. However, when using OOB channel, if the onboard BIOS or the BIOS firmware image does not support OOB functions, the DMI information, such as MB serial number, might get lost after system reboot.
- If Feature Toggled On is No, all licensed features will be turned OFF and Node Product Key Activated will be N/A.

Known Limitations:

- If we roll back BIOS from OOB-supported version to non-supported version, the information for "BIOS build date" and "OOB support in BIOS" fields will not be changed accordingly.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c CheckOOBSupport
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c CheckOOBSupport
```

In-band:

```
[SUM_HOME]# ./sum -c CheckOOBSupport
```

The console output contains the following information.

```
[KEY]
Node Product Key Format.........JSON
Node Product Key Activated.......OOB
    SFT-DCMS-SVC-KEY Activated...Yes
Feature Toggled On..............YES

[BMC]
BMC FW Version..................02.41
BMC Supports OOB BIOS Config.....Yes
BMC Supports OOB DMI Edit........Yes

[BIOS]
BIOS Board ID...................0660
BIOS Build Date.................2013/9/18
BIOS Supports OOB BIOS Config....Yes
BIOS Supports OOB DMI Edit.......Yes

[SYSTEM]
System Supports RoT Feature......Yes
```

5.2.2 Checking Asset Information (OOB Only)

Use the command “CheckAssetInfo” to check the asset information for the managed system. On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, the add-on devices are displayed by the riser cards to which they are connected.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c CheckAssetInfo
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c CheckAssetInfo
```

The console output is different on different platforms. Examples are provided below.

On platforms before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets

```
Supermicro Update Manager (for UEFI BIOS) 2.2.0 (2018/12/27) (x86_64)
Copyright(C)2018 Super Micro Computer, Inc. All rights reserved.

System
======
    Product Name: SuperPN
    Product PartModel Number: SYS-1028U-E1CR4+-1-WM001
    Version: 0123456789
    Serial Number: SuperSN
    UUID: 00000000-0000-0000-0000-0CC47A3A4094

Baseboard
=========
    Product Name: SuperBPN
    Version: 1.00
    Serial Number: CM144S013179

CPU
===
    [CPU(1)]
            Family: Intel® Xeon® processor
            Manufacturer: Intel(R) Corporation
            Version: Intel(R) Genuine processor
            Current Speed: 1800 MHz
            Enabled Cores: 12
```

```
            Total Cores: 12
            CPU ID: 52 06 05 00 ff fb eb bf
    [CPU(2)] N/A


Memory
======
    [MEM(1)] N/A
    [MEM(2)] N/A
    [MEM(3)] N/A
    [MEM(4)] N/A
    [MEM(5)] N/A
    [MEM(6)] N/A
    [MEM(7)] N/A
    [MEM(8)] N/A
    [MEM(9)] N/A
    [MEM(10)] N/A
    [MEM(11)]
             Locator: P1-DIMMF1
             Manufacturer: SK Hynix
             Manufacturing Date (YY/WW): 14/05
             Part Number: HMA41GR7MFR4N-TFT1
             Serial Number: 101E19A4
             Size: 8192 MB
             Current Speed: 2133 MHz
    [MEM(12)] N/A
    [MEM(13)] N/A
    [MEM(14)] N/A
    [MEM(15)] N/A
    [MEM(16)] N/A
    [MEM(17)] N/A
    [MEM(18)] N/A
```

```
    [MEM(19)] N/A
    [MEM(20)] N/A
    [MEM(21)] N/A
    [MEM(22)] N/A
    [MEM(23)] N/A
    [MEM(24)] N/A


Add-on Network Interface
==================================
    [NIC(1)]
              Device Class: Network controller
              Device Subclass: Ethernet controller
              Vendor: Intel Corporation (ID:8086)
              Subvendor: Super Micro Computer, Inc. (ID:15D9)
              Device Name:  (ID:1583)
              Subsystem Name:  (ID:0000)
              Serial Number: VA168S018887
              Part Number: AOC-S40G-i2Q

              MAC Address1: 0CC47A1971AA
              Current Speed: 1000Mb/s

              MAC Address2: 0CC47A1971AB
              Current Speed: 1000Mb/s

              Slot Location: 1
              Slot Type: SBX3 (Riser)
```

```
Add-on PCI Device
===================================
    [Device(1)]
              Device Class: Network controller
              Device Subclass: Ethernet controller
              Vendor: Intel Corporation (ID:8086)
              Subvendor: Super Micro Computer, Inc. (ID:15D9)
              Device Name:  (ID:1583)
              Subsystem Name:  (ID:0000)

              Slot Location: 1
              Slot Type: SBX3 (Riser)



Onboard Network Interface
===================================
    [NIC(1)]
              Device Class: Network controller
              Device Subclass: Ethernet controller
              Vendor: Intel Corporation (ID:8086)
              Subvendor: Super Micro Computer, Inc. (ID:15D9)
              Device Name:  (ID:1528)
              Subsystem Name: AOC-UR-i2XT (ID:085D)
              Serial Number: N/A
              Part Number: N/A
              MAC Address: N/A

              Device Status of LAN1: Enabled
              Device Type of LAN1: Ethernet
              Reference Designation of LAN1: Intel Ethernet X540 #1
```

```
            Device Status of LAN2: Enabled
            Device Type of LAN2: Ethernet
            Reference Designation of LAN2: Intel Ethernet X540 #2


Onboard PCI Device
==================================
    [Device(1)]
            Device Class: Display controller
            Device Subclass: VGA controller (VGA compatible controller)
            Vendor: ASPEED Technology Inc. (ID:1A03)
            Subvendor: Super Micro Computer, Inc. (ID:15D9)
            Device Name:  (ID:2000)
            Subsystem Name:  (ID:091C)

            Device Status of Video1: Enabled
            Device Type: Video
            Reference Designation of Video1: ASPEED Video AST2500

    [Device(2)]
            Device Class: Network controller
            Device Subclass: Ethernet controller
            Vendor: Intel Corporation (ID:8086)
            Subvendor: Super Micro Computer, Inc. (ID:15D9)
            Device Name:  (ID:1528)
            Subsystem Name: AOC-UR-i2XT (ID:085D)

            Device Status of LAN1: Enabled
            Device Type of LAN1: Ethernet
            Reference Designation of LAN1: Intel Ethernet X540 #1
```

```
            Device Status of LAN2: Enabled
            Device Type of LAN2: Ethernet
            Reference Designation of LAN2: Intel Ethernet X540 #2


System Network Interface
====================================
    [LAN(1)]
            MAC Address: 0CC47A3A4094
            Current Speed: 1000Mb/s
    [LAN(2)]
            MAC Address: 0CC47A3A4095
            Current Speed: 1000Mb/s

IPMI Network Interface
====================================
    [IPMI]
            MAC Address: 0CC47A685A67
```

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, output of add-on sections is different from previous example. The example is shown below.

```
Add-on Network Interface
====================================
    [[[SXB3 (Riser)]]]
        [[Onboard]]
            [NIC(1)]
                    Device Class: Network controller
                    Device Subclass: Ethernet controller
                    Vendor:  (ID:1528)
                    Subvendor: AOC-UR-i4XT (ID:0847)
```

```
        Device Name: Intel Corporation (ID:8086)
        Subsystem Name: Super Micro Computer, Inc. (ID:15D9)
        Serial Number: OA182S021066
        Part Number: AOC-UR-i4XT

        MAC Address1: AC1F6B0FEA62
        Current Speed1: 0Mb/s

        MAC Address1: AC1F6B0FEA63
        Current Speed1: 0Mb/s

        Slot Number: Onboard
        Slot Designation: SXB3


[NIC(2)]
        Device Class: Network controller
        Device Subclass: Ethernet controller
        Vendor:  (ID:1528)
        Subvendor: AOC-UR-i4XT (ID:0847)
        Device Name: Intel Corporation (ID:8086)
        Subsystem Name: Super Micro Computer, Inc. (ID:15D9)
        Serial Number: OA182S021066
        Part Number: AOC-UR-i4XT

        MAC Address2: AC1F6B0FEA64
        Current Speed2: 1000Mb/s

        MAC Address2: AC1F6B0FEA65
        Current Speed2: 0Mb/s
```

```
                    Slot Number: Onboard
                    Slot Designation: SXB3


        [[AOC(1)]]
            [NIC(1)]
                    Device Class: Network controller
                    Device Subclass: Ethernet controller
                    Vendor:  (ID:1583)
                    Subvendor:  (ID:0000)
                    Device Name: Intel Corporation (ID:8086)
                    Subsystem Name: Super Micro Computer, Inc. (ID:15D9)
                    Serial Number: VA168S018887
                    Part Number: AOC-S40G-i2Q

                    MAC Address1: 0CC47A1971AA
                    Current Speed1: 0Mb/s

                    MAC Address1: 0CC47A1971AB
                    Current Speed1: 0Mb/s

                    Slot Number: 1
                    Slot Designation: AOC-UR-i4XT SLOT1 PCI-E 3.0 X8



Add-on PCI Device
==================================
    [[[SXB3 (Riser)]]]
        [[Onboard]]
            [Device(1)]
```

```
                Device Class: Network controller
                Device Subclass: Ethernet controller
                Vendor:  (ID:1528)
                Subvendor: AOC-UR-i4XT (ID:0847)
                Device Name: Intel Corporation (ID:8086)
                Subsystem Name: Super Micro Computer, Inc. (ID:15D9)

                Slot Number: Onboard
                Slot Designation: SXB3


    [Device(2)]
                Device Class: Network controller
                Device Subclass: Ethernet controller
                Vendor:  (ID:1528)
                Subvendor: AOC-UR-i4XT (ID:0847)
                Device Name: Intel Corporation (ID:8086)
                Subsystem Name: Super Micro Computer, Inc. (ID:15D9)

                Slot Number: Onboard
                Slot Designation: SXB3


[[AOC(1)]]
    [Device(1)]
                Device Class: Network controller
                Device Subclass: Ethernet controller
                Vendor:  (ID:1583)
                Subvendor:  (ID:0000)
                Device Name: Intel Corporation (ID:8086)
                Subsystem Name: Super Micro Computer, Inc. (ID:15D9)
```

```
Slot Number: 1
Slot Designation: AOC-UR-i4XT SLOT1 PCI-E 3.0 X8
```

Notes:

- Items supported only since X10 Intel® Xeon® Processor E5 v3/v4 Product Family platform and selected systems are: System: Version, UUID, CPU, BaseBoard, Memory, and Add-on Network Interface.
- Items supported only since X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets platform and selected systems: Onboard Network Interface, Add-on PCI Device, and Onboard PCI Device.
- Items generally supported are: System: Product Name, Serial Number, System Network Interface, and IPMI Network Interface.
- Current Speed in Network Interface requires TAS installation in the managed system.
- For riser card chips, its device information will be listed in the add-on card section and under the label “Onboard”.

5.2.3 Checking Sensor Data (OOB Only)

Use the command “CheckSensorData” to check the sensor data for the managed system.

Notes:

- Supported sensors vary from different motherboards and firmware images.
- Network add-on card temperature can be retrieved from some X10 or later systems.
- For PS and Chassis Intrusion sensors, the “Reading” field is only used to debug. You only need to check if the “Status” field shows “OK”.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c CheckSensorData
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c CheckSensorData
```

For CPU temperature sensor, the console output contains the following information.

```
Status | (#)Sensor                |      Reading | Low Limit | High Limit |
------ | ---------                |      ------- | --------- | ---------- |
OK     | (4) CPU Temp             |     48C/118F |       N/A |   97C/207F |
```

5.2.4 Checking System Utilization (OOB Only)

Use the command “CheckSystemUtilization” to check the device utilization status for the managed system.

Notes:

- This command requires a TAS agent to collect the system statuses. If a TAS agent is not installed on the managed system, the system statuses will be shown as N/A.
- The OS of the managed system must be booted for the TAS agent to collect the real-time device utilization.
- This command is supported since X10 platforms and select systems.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c CheckSystemUtilization
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c
CheckSystemUtilization
```

The console output contains the following information.

```
Time
====
    Last Sample Time: 2014-05-16_17:16:02

OS
==
    OS Name: RedHatEnterpriseServer
    OS Version: 6.4 x86_64

CPU
===
    CPU Utilization: 2.74 %

Memory
======
    Memory Utilization: 8 %
```

```
LSI(1)
======
    HDD Name: /dev/sdb
    Slot number: 1
    SMART Status: Ok

HDD(1)
======
    HDD name: /dev/sda
    SMART Status: Ok
    Serial number: Z2AABXL3
    Total Partitions: 2
    [Partition(1)]
            Partition Name: /dev/sda1
            Utilization: N/A
            Used Space: N/A
            Total Space: 17.58 GB
    [Partition(2)]
            Partition Name: /dev/sda2
            Utilization: 22.01 %
            Used Space: 3.62 GB
            Total Space: 17.30 GB


RSTe(1)
======
    Volume name: /dev/md126
    Controller name: Intel RSTe
    Numbers of Drives: 2
     [HDD(1)]
            HDD name: /dev/sdc
            SMART Status: Ok
     [HDD(2)]
            HDD name: /dev/sdd
```

```
            SMART Status: Ok

Network
=======
    Total Devices: 2
    [NIC(1)]
            Device Name: eth0
            Utilization: <1 %
            Status: up
    [NIC(2)]
            Device Name: eth1
            Utilization: 0 %
            Status: down
```

Notes:

- RAID Device type LSI, RSTe and NVMe shows only if they have been installed on the host machine.
- When RSTe Device is installed on the host machine, normal Hard Disk type (HDD) information will not display.

5.2.5 ServiceCalls

Use the command "ServiceCalls" to check the system event log and sensor data record of the managed system with the ServiceCalls configuration file. After the execution, the recipients assigned in the file will receive SEL and SDR reports by e-mail.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ServiceCalls --file
<servicecalls XML file>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ServiceCalls --file
servicecalls_sample.xml
```

In-Band:

```
[SUM_HOME]# ./sum -c ServiceCalls --file servicecalls_sample.xml
```

5.2.5.1 ServiceCalls XML File Format

A ServiceCalls XML file is composed of several nodes, and each node is explained below. For a complete example of a ServiceCalls XML file, you can find one file names as "servicecalls_sample.xml" bundled in the SUM release package.

- SMTP Server Node - <SMTPServer> (Required)

  To fill out your e-mail server information, SMTP server information is required. The sub-node

  ServerURI is the full SMTP URI, and ServerPort is the SMTP port on your SMTP server, which along

  with SMTP SSL and SMTP STARTTLS are supported by SUM. SUM is known to support ports 25, 465 and 587. Also,you need to provide the sender's information such as their e-mail address, ID, and password for e-mails.
- Trigger Items Node - <Trigger_Items>

You can select the trigger item types you plan to monitor. There are three sub-nodes: SDR_Trigger_Items, SEL_Trigger_Items and HW_Event_Alert.

- SDR_Trigger_Items

  SDR (Sensor Data Records) records information of types and numbers of sensors in the managed platform. You can enable or disable this function.

- SEL_Trigger_Items

  There are three types of events detected by the managed system in the SEL (System Event Log): critical, warning, and information. Types of SEL events include “Disk SMART failure”, “CATERR”, “Uncorrectable ECC”, “Bus Fatal Error”, and so on.The SEL items are all listed in “servicecalls_example.xml”. To decide how an SEL node is to be monitored, you can set it to “Trigger” or “Skip”.

- HW_Event_Alert

  HW-related events on the managed system, including SDR and SEL, are monitored. Types of SDR events are “FAN mode” and “Power Unit Status”. Types of SEL events include “Memory”, “Drive Slot”, “Bus Fatal Error”, “DIMM Error”, and so on. If “Notification” is set to “Enable” and the receipient’s e-mail address (“RecipientEmail”) is genunine and correct, the status of HW events will be sent to the recipient’s e-mail address. The default “RecipientEmail” e-mail is “hwevent_alert@supermicro.com”.

- Recipient Information node - <Recipient_Information> (Required)

  This section allows user to fill out the recipient’s information, such as his/her name (“Name”) and his/her title (“Role”) in each node, and set the recipient’s e-mail addresss in the node to receive alerts classified as non-HW events.

- Customer Information node - <Customer_Information>

  You can fill out the information of the customer applying for ServiceCalls service, such as name and company.

- Site Location Information node - <Site_Location_Information>

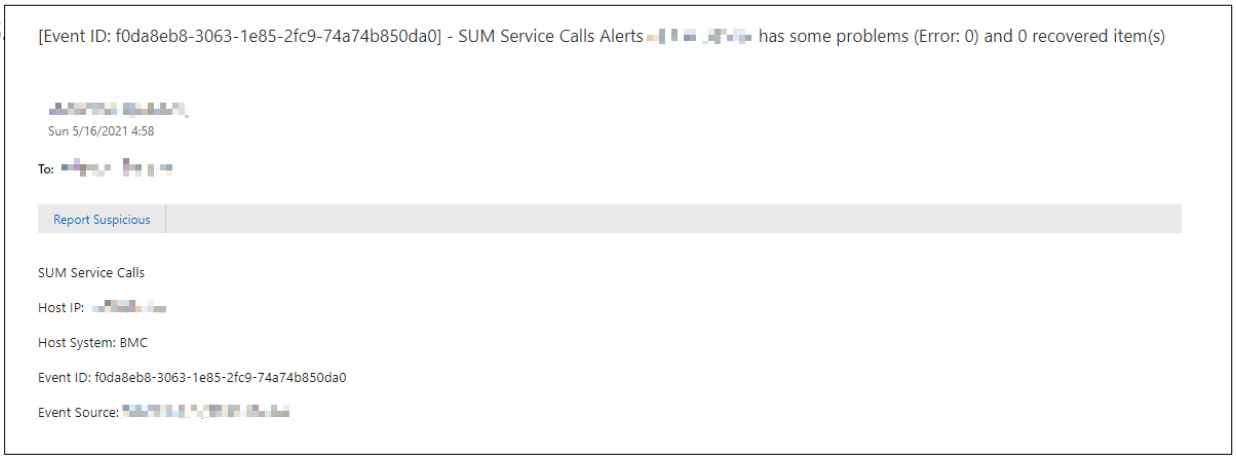
  You can mention where the managed system is located. Besides company name and address, the contact information can be filled out for further action.

Notes:

- Only the contents of each attribution and node can be edited.
- The content of attribution must be quoted with double quotes.
- The SMTP URI in the content of <ServerURL > requires an SMTP scheme. If SMTP is set, it should be “smtp://<SMTP server path>.” If SMTP SSL is set, it should be “smtps://<SMTP server path>.”
- If the SMTP scheme is “smtps”, please make sure your SMTP server’s SSL is open, and the certification is not expired.

E-mail Format

5.2.5



The e-mail content includes:

- **Subject Line**

  Contains Event ID, function name, the managed system BMC/CMM IP, and the summary of the host.

- **Body**
  - **E-mail Function**: It is “SUM Service Calls” in this example.
  - **Host IP**: The BMC/CMM IP address of the managed system.
  - **Event ID**: The 32 bytes of GUID.
  - **Event Source**: The OS IP address of the managing system.
- **Problematic Items**:

If SEL and SDR trigger items are problematic, they will be categorized in this group. For SEL problems, each item includes index, severity, timestamps, sensor type and description. The value [NEW] is used to indicate this item is new.

- **User-Defined Event E-mail**:

  The SEL problem consists of three severity levels: “critical”, “warning” and “information", which is defined by SUM. The SDR items exceeding their thresholds will be treated as problematic items.

```
[Problematic Items]
Index, Severity, TimeStamp, Sensor Type, Description
1, CRITICAL, 2020/12/10 17:20:33, HDD_OEM, Disk120 SMART failure [NEW]
2, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEM EVENT GH [NEW]
3, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEM EVENT GH [NEW]
4, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEM EVENT EF [NEW]
5, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEM EVENT EF [NEW]
6, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEM EVENT CD [NEW]
7, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEM EVENT CD [NEW]
8, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEM EVENT AB [NEW]
9, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEM EVENT AB [NEW]
10, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, PROCHOT P2
11, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, PROCHOT P1
12, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEMCHOT P2
13, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEMCHOT P2
14, CRITICAL, 2020/12/10 17:20:33, CPLD_OEM, MEMCHOT P1
```

- **HW Event Alert E-mail**:

  HW-related events of SEL and SDR all appear as “Critical.”

```
[Problematic Items]
Index, Severity, TimeStamp, Sensor Type, Description
1, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, CATERR [NEW]
2, CRITICAL, 2020/10/29 20:31:24, BIOS_OEM_Memory_Error, Uncorrectable error found, Memory Rank is disabled. (P1-DIMMC3) [NEW]
3, CRITICAL, 2020/10/29 20:31:24, BIOS_OEM_Memory_Error, Failing DIMM: DIMM location (Uncorrectable memory component found). (P1-DIMMC3) [NEW]
4, CRITICAL, 2020/10/29 20:31:24, BIOS_OEM_Memory_Error, DIMM mapped out (P1-DIMMC3) [NEW]
5, CRITICAL, 2020/10/29 20:31:24, NVMe_OEM, NVMeBPN @ 160 Group @ 0 Slot @ 15: Drive fault [NEW]
6, CRITICAL, 2020/10/29 20:31:24, Processor_Configuration_OEM, Bus Fatal Error CPUSocket#0, BankType:IFU [NEW]
7, CRITICAL, 2020/10/29 20:31:24, Management_Subsystem_Health, Controller access degraded or unavailable [NEW]
8, CRITICAL, 2020/10/29 20:31:24, Battery, Battery failed [NEW]
9, CRITICAL, 2020/10/29 20:31:24, Memory, Uncorrectable ECCP4-@DIMMO6(CPU4) [NEW]
10, CRITICAL, 2020/10/29 20:31:24, OEM_DRIVER_SLOT, Drive Fault @ PDSlot10 [NEW]
11, CRITICAL, 2020/10/29 20:31:24, OEM_DRIVER_SLOT, Drive Fault @physical slot10 [NEW]
```

- **Recovered Items (Last Check)**:

  This section contains the SEL and SDR items previously marked as problematic items but later recovered in the last check.

```
[Recovered Items (Last Check)]
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, HDD_OEM, Disk120 SMART failure
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT GH
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT GH
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT EF
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT EF
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT CD
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT CD
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT AB
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT AB
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, PROCHOT P2
[#Recovered from Event ID:96b96d44-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, PROCHOT P1
```

- **Summary**:

The number of both problematic and recovered items are shown in the Summary.

```
[Summary]
 <Critical items>: 46
 <Warning items>: 10
 <Information items>: 5
 <Recovered items>: 61
```

- **Additional Items**:

  User-Defined Event Email and HW Event Alert E-mail are different, but both include status, timestamps, sensor type, reading, and threshold.

  - **User-Defined Event E-mail**: This section contains the normal status of SDR items.

```
[Additional Items]
Status, TimeStamp, Sensor Type, Reading, Low Limit, High Limit
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, CPU1 Temp, 37C/99F, 5C/41F, 99C/210F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, CPU2 Temp, N/A, N/A, N/A
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, PCH Temp, 39C/102F, 5C/41F, 90C/194F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, System Temp, 29C/84F, 5C/41F, 85C/185F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, Peripheral Temp, 34C/93F, 5C/41F, 85C/185F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, MB_NIC_Temp1, 41C/106F, 5C/41F, 100C/212F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, MB_NIC_Temp2, N/A, N/A, N/A
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, VRMCpu1 Temp, 30C/86F, 5C/41F, 100C/212F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, VRMCpu2 Temp, N/A, N/A, N/A
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, VRMP1ABC Temp, 36C/97F, 5C/41F, 100C/212F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, VRMP1DEF Temp, 34C/93F, 5C/41F, 100C/212F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, VRMP2ABC Temp, N/A, N/A, N/A
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, VRMP2DEF Temp, N/A, N/A, N/A
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, FAN1, 900 RPM, 500 RPM, 25400 RPM
```

  - **HW Event Alert E-mail**: This section contains both SEL and SDR items, including Problematic and non-Problematic events.

```
[Additional Items]
Status, TimeStamp, Sensor Type, Reading, Low Limit, High Limit
1, CRITICAL, 2020/10/29 20:31:24, HDD_OEM, Disk120 SMART failure
2, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, MEM EVENT GH
3, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, MEM EVENT GH
4, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, MEM EVENT EF
5, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, MEM EVENT EF
6, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, MEM EVENT CD
7, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, MEM EVENT CD
8, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, MEM EVENT AB
9, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, MEM EVENT AB
```

- **Device Info**:

```
[Device Info]
 <Motherboard>
  Asset Tag: Base Board Asset Tag
  Motherboard Model Name: X12DPi-N6
  Motherboard Model Version: 1.00
  Motherboard Serial Number: UM208S003679
 <System>
  System Product Name:
  System Product Part Model Number:
  Version: 123456789
  Serial Number:
  UUID: 28AC7E00-E139-11EA-8000-3CECEF2C6DBE
 <Product Keys>
  SFT-OOB-LIC        , creation date: 2020/11/12
  SFT-DCMS-SINGLE , creation date: 2020/11/12
  SFT-DCMS-SVC-KEY, creation date: 2020/11/20
```

This section displays BMC or CMM hardware information including "Motherboard", "System," and "Product Key" on the managed system. Note that the device configuration determines what information from the managed system you obtain.

Note: Both node product keys, "SFT-DCMS-SINGLE" and "SFT-DCMS-SVC-KEY", are required to execute this command.

- **Site Location Info**:

```
[Site Location Info]
 Company: PeterT Comp
 Address: 980 Rock Avenue
 City: San Jose
 State/Province: CA
 Zip: 95131
 Country: US
 Contact Person: Peter Tsai, Admin
                 Email: PeterTsai@supermicro.com.tw
```

The location where the managed system is located.

- **Customer Info**:

```
[Customer Info]
 Company: PohanL Inc.
 Contact Person: Pohan Lu
                 Email: PohanL@supermicro.com.tw
```

The customer who owns the managed system.

Cache File

5.2.5.3

After running the ServiceCalls command, a file named "**.servicecalls.cache.db**" will be generated under the execution folder. We implement database to manage the SEL/SDR/HW events. The cache file is designed to update the events status of host. The file will be read every time the command executed and compare the the events' status of the current with those in the file. If events status are recovered or generated, we will update the file and send E-mail with the latest status at the end of execution.You can change the cache file location in the .sumrc file. For details, see *4.1 Customizing SUM Configurations*. The execution history, including e-mail contents and e-mail sender/recipient information, are saved in a database file for SUM internal reference. If you remove the database file, a new one will be generated after the command is executed again. Note that all previous problematic events will be treated as new events.

Known Limitations:

- SUM cannot access cache files on mounted file systems.

5.3 BIOS Management for a Single System

5.3.1 Getting BIOS Firmware Image Information

Use the command "GetBiosInfo" to receive the BIOS firmware image information from the managed system as well as the local BIOS firmware image (with option --file).

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetBiosInfo [--file
<filename> [--file_only]] [--showall]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBiosInfo --file
SMCI_BIOS_signed.rom
```

The console output contains the following information when secure flash is signed from local BIOS image.

```
Managed system.....192.168.34.56
    Board ID.....0660
    BIOS build date......2012/10/17
Local BIOS image file.... SMCI_BIOS_signed.rom
    Board ID.....0988
    BIOS build date......2018/5/7
    FW image.....Signed
        Signed Key.......SecureFlash
```

In-Band:

```
[SUM_HOME]# ./sum -c GetBiosInfo --file SMCI_BIOS_signed.rom --file_only
```

The console output contains the following information when RoT is signed from local BIOS image.

```
Local BIOS image file....SMCI_BIOS_signed.rom
    Board ID.....1B6A
```

```
    BIOS build date......2021/01/12
    FW image.............Signed
        Signed Key.......RoT
```

```
[SUM_HOME]# ./sum -c GetBiosInfo --file SMCI_BIOS.rom --showall
```

The console output contains the following information.

```
Managed system...........192.168.34.56
    Board ID.............0660
    BIOS build date......2012/10/17
    BIOS version.........1.0
    BIOS revision........1.8
Local BIOS image file.... SMCI_BIOS.rom
    Board ID.............1B4A
    BIOS build date......2021/03/11
    FW image.............Signed
        Signed Key.......RoT
    BIOS version.........1.0a
    BIOS revision........5.22
    FW global version: 0
    RC version: 20.P80
    SPS version: 4.4.4.53
    CPU signature: 00 06 06 a4
    Description: IceLakeServer L0
    Version: 0B000280
    CPU signature: 00 06 06 a5
    Description: IceLakeServer C0
    Version: 0C0002B0
    CPU signature: 00 06 06 a6
    Description: IceLakeServer D0
    Version: 0D000260
```

```
.............
BIOS build date: 2021/03/11
BIOS version: 1.0a
UUID: 936B704B-2D82-EB11-9FAD-0CC47AFBDDC6
PMEM version: 02.02.00.1553
BIOS unique name: BIOS_X12SPI-1B4A_20210311_1.0a_STDsp.bin
```

SecureFlash-signed key of local BIOS image displays the following information:

Type	Description
Signed	Secure flash is signed by Super Micro Computer, Inc.
Signed(U)	Secure flash is NOT signed Super Micro Computer, Inc., but by unknown authority.
(Not shown)	The "FW image" field is not shown because of no secure flash signed in the image.

RoT-signed key of local BIOS image displays the following information:

Type	Description
Signed	RoT is signed by Super Micro Computer, Inc.
Signed(C)	RoT is verified by the specified certificate.
Signed(U)	RoT is NOT signed by Super Micro Computer, Inc. but by an unknown authority.
Verification failed	The RoT signing in the image cannot be verified because the image is corrupted or incomplete.

Notes:

- BIOS secure flash and RoT signed information are supported.
- The PMem firmware version in this section is the BIOS built-in PMem firmware version.

5.3.2 Updating the BIOS Firmware Image

Use the command "UpdateBios" with BIOS firmware image SMCI_BIOS.rom to run SUM to update the managed system.

For X12/H12 and later RoT platforms, in-band BIOS update can only be done through Redfish Host Interface. For details, refer to *4.10 Redfish Host Interface*. SUM powers off the system after uploading BIOS firmware image, and automatically powers on the system after BIOS is updated.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
UpdateBios --file <filename> [options…]
```

Option Commands	Descriptions
--reboot	Forces the managed system to reboot or power up after operation.
--flash_smbios	Overwrites and resets SMBIOS data.
--preserve_mer	Preserves the ME firmware region.
--preserve_nv	Preserves NVRAM.
--kcs	Updates BIOS through KCS. (Only in-band usage is supported.)
--preserve_setting	Preserves BIOS configurations.
--erase_OA_key	Erases OA key. (Only in-band usage is supported.)
--policy <policy filename>	Updates the BIOS based on the given policy file. (Only multiple systems OOB usages are supported.)
--precheck	Works with the option –policy. Note that this option only shows the parsing results without updating BIOS.
--backup	Backs up the current BIOS image. (Only supported by the RoT systems.)
--forward	Confirms the Rollback ID and upgrades to the next revision. (Only supported by the X12/H12 and later platforms except the H12 non-RoT systems.)
--post_complete	Wait for the managed system POST to complete after reboot.
--clear_password	Clears BIOS password.
--erase_secure_boot_key	Erases secure boot key.
--reset_boot_option	Resets BIOS boot configurations.

Notes:

- Before performing the OOB UpdateBios command, it is recommended to shut down the managed system first.

- When doing in-band UpdateBios command, SUM will disable watchdog and unload me/mei driver from the OS if it exists.
- With the Server ME embedded on the Supermicro system, you may encounter a problem executing the in-band SUM command "UpdateBios" when the Client ME driver (MEIx64) is installed on the Windows platform. To prevent the system from hanging, you need to remove the driver before updating BIOS. The steps are displayed upon detection.
- When using SSH connection to do in-band UpdateBios command, SSH timeout on both client and server side should be adjusted to avoid broken pipe during command execution. Typical execution time is within 30 minutes. Timeout value should be longer than 30 minutes.
- If the updated BIOS FDT (Flash Descriptor Table) is different from the current BIOS FDT or if ME protection needs to be disabled when the in-band UpdateBios command is executed, a warning message stating necessary actions is displayed.
- When multiple boot is installed, we should use default boot OS to run this command so that when FDT is different, the jumper-less solution can continue updating BIOS after the first reboot.
- OOB UpdateBios command has not been supported for MBs that implemented client ME such as X11SAE-F, X11SAT-F, X11SSZ-(Q)F/LN4F, X11SBA-(LN4)F and C7-series.
- X9DRL-3F/-iF MB does not support OOB update BIOS and OOB/In-band DMI information related commands.
- Signed BIOS update is supported.
- The --reboot option is required for X12/H12 and later ROT platforms.
- The --backup option backs up the current BIOS image on the managed system, not the BIOS file to be updated.
- The --backup option only supported by the X12/H12 and later RoT platforms.
- Due to the known issue of GRUB2 loader, the system may not be able to boot and hangs up after BIOS update is upgraded. If the version of GRUB2 loader is not the lastest, please downgrade BIOS to the previous version and upgrade GRUB2 loader to the latest version. Then perform BIOS upgrade to the target BIOS again. For more details, please refer to the FAQ on the Supermicro web site, https://www.supermicro.com/support/faqs/faq.cfm?faq=33400.

Example:

OOB :

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBios --file
SMCI_BIOS.rom --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c UpdateBios --file SMCI_BIOS.rom --reboot
```

In-Band through KCS:

```
[SUM_HOME]# ./sum -c UpdateBios --file SMCI_BIOS.rom --kcs --reboot
```

In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateBios --file
SMCI_BIOS.rom --reboot
```

Notes:

- The OOB usage of this function is available when the BMC node product key is activated.
- The in-band usage of this function does not require node product key activation.
- The firmware image can be successfully updated only when the board ID of the firmware image and the managed system are the same.
- You have to reboot or power up the managed system for the changes to take effect.
- When using an OOB channel, if the onboard BIOS or the BIOS firmware image does not support OOB functions, the DMI information, such as the motherboard serial number, might be lost after system reboot.
- DO NOT flash BIOS and BMC firmware images at the same time.
- --preserve_nv and --flash_smbios options cannot be used at the same time.
- --flash_smbios option is used to erase and restore SMBIOS information as factory default values. Unless you are familiar with SMBIOS data, do not use this option.
- --preserve_nv option is used to preserve BIOS NVRAM data. Unless you are familiar with BIOS NVRAM, do not use this option.
- --preserve_mer option is used to preserve ME firmware region. Unless you are familiar with ME firmware region, do not use this option.
- --preserve_setting option requires SFT-OOB-LIC key (both OOB and In-Band) and it is only supported on X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms. The preserved setting configurations will be listed in a preserved_settings.log. Another way to know which BIOS setting is preserved is to run the commands GetCurrentBioscfg and GetDefaultBioscfg after BIOS updated. Compare the two files and the different values between these two files are the preserved settings.
- The firmware verification to update the BMC is supported. SUM prevents the BMC from being updated with unauthorized firmware.

5.3.3 Receiving Current BIOS Settings

Use the command "GetCurrentBiosCfg" to execute SUM to get the current BIOS settings from the managed system and save it in USER_SETUP.file.

Notes:

- This BIOS configuration file is synchronized to the BMC from the BIOS when the system reboots or powers up.
- If the customer has flashed BMC firmware image, this function will not work until the managed system is first rebooted or powered up.
- X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and newer platforms support HII. The current BIOS settings will be generated as XML and plain text formats for HII and DAT respectively.
- The XML file of BIOS configuration contains extended ASCII characters. Please use ISO 8859-1 encoding to view BIOS configuration XML file.
- SUM 2.2.0 or later supports text-based user interface. For details, refer to *4.9 TUI.*
- SUM 2.7.0 or later supports generating a compact version of BIOS configuration file for TUI using "--compact" option to remove the unchanged BIOS settings. To view an example of a compact configuration file, refer to *Appendix G. Removing Unchanged BIOS Settings in an XML File*.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetCurrentBiosCfg --
file <USER_SETUP.file> [--overwrite] [--tui [--compact]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCurrentBiosCfg --
file USER_SETUP.file --overwrite
```

In-Band:

```
[SUM_HOME]# ./sum -c GetCurrentBiosCfg --file USER_SETUP.file --overwrite
```

5.3.4 Updating BIOS Settings Based on the Current BIOS Settings

1. Follow the steps in *5.3.3 Receiving Current BIOS Settings*.

2. Edit the item/variable values in the user setup text file USER_SETUP.file to the desired values as illustrated in *4.3 Format of BIOS Settings Text File* (for DAT) or *4.4 Format of BIOS Settings XML File* (for HII).
3. Remove unchanged settings/menus in the BIOS configuration file. Note that this step is optional. For details, see *Appendix G. Removing Unchanged BIOS Settings in an XML File*.
4. Use the command "ChangeBiosCfg" with the updated file USER_SETUP.file to run SUM to update the BIOS configuration.

Notes:

- The editable BIOS configuration items may be changed for different BIOS versions. Please make sure the BIOS configurations are consistent with the BIOS version on the managed system.
- The uploaded configuration will only take effect after a system reboot or power up.
- For HII, when the new BIOS firmware image is flashed, there may be conflicts between the BIOS configuration file and the latest BIOS configuration in the managed system. The current BIOS configuration file should be re-downloaded, re-modified and then updated.
- When hardware resources or settings are changed, a previously downloaded BIOS configuration file may become outdated. When a BIOS configuration file is inconsistent with the latest BIOS configuration in the managed system, using the options --skip_unknown and--skip_bbs (both options are only supported in HII) may solve the problem.

  For instance, when an AOC has been removed from the managed system, the BIOS configuration for the related menus or settings may become invalid. The option --skip_unknown is designed to skip all invalid menus and settings in the latest BIOS configuration in the managed system.

  In another example, when a hard disk device is changed, the option string in the Option setting in the BBS related menus may become invalid as well. The option --skip_bbs is designed to skip all BBS related menus. The "related BBS menu" is defined as owning "Priorities" in its name and "Boot" for its parent menu.
- For X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, the same boot device may be presented with slightly varied boot strings. BIOS/SUM concludes that the boot type and port location can be used for identifcation. For example, a UEFI boot device mounted at port 0 can be represented as "UEFI P0: Hard disk A0001", "UEFI P0: Hard disk A0002" and "UEFI P0". "A0001" and "A0002" can be two identical hard disks with different serial numbers, and there is no boot device information in the default BIOS configuration for "UEFI P0". When SUM can't match the whole boot option string, it will try to match the substring before the first colon. For example, "UEFI P0: Hard disk A0001" matches "UEFI P0: Hard disk A0002" and "UEFI

P0".

- The BIOS configuration XML file contains extended ASCII characters. Use ISO 8859-1 encoding to view and save BIOS configurations in an XML file.
- From SUM 2.5.0, a BIOS configuration tagged with "<LicenseRequirement>" requires the SFT-DCMS-SINGLE node product key to change the BIOS setting. Please refer to *Appendix E.6 License Requirement Setting* for more details.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ChangeBiosCfg --file
<USER_SETUP.file> [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeBiosCfg --file
USER_SETUP.file --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c ChangeBiosCfg --file USER_SETUP.file –reboot
```

5.3.5 Receiving Factory BIOS Settings

Use the command "GetDefaultBiosCfg" to execute SUM to get the default factory BIOS settings from the managed system and save it in the USER_SETUP.file file.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetDefaultBiosCfg --
file <USER_SETUP.file> [--overwrite]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetDefaultBiosCfg --
file USER_SETUP.txt --overwrite
```

In-Band:

```
[SUM_HOME]# ./sum -c GetDefaultBiosCfg --file USER_SETUP.file --overwrite
```

5.3.6 Updating BIOS Settings Based on the Factory Settings

1. Follow the steps in *5.3.5 Receiving Factory BIOS Settings*.
2. Follow steps 2 to 4 in *5.3.4 Updating BIOS Settings Based on the Current BIOS Settings*.

5.3.7 Loading Factory BIOS Settings

Use the command LoadDefaultBiosCfg to execute SUM to reset the BIOS settings of the managed system to the factory default settings.

Note: The uploaded configuration will take effect only after a reboot or power up.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c LoadDefaultBiosCfg [--
reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c LoadDefaultBiosCfg --
reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c LoadDefaultBiosCfg --reboot
```

5.3.8 Receiving DMI Information

Use the command "GetDmiInfo" to execute SUM to get the current supported editable DMI information from the managed system and save it in the DMI.txt file.

Notes:

- This DMI file is synchronized to BMC from BIOS when the system reboots or powers up.
- If the customer has flashed BMC firmware image, this function will not work until the managed system is first rebooted or powered up.
- The supported editable DMI items could vary from BIOS to BIOS. SUM will only show supported items.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetDmiInfo --file
<DMI.txt>  [--overwrite]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetDmiInfo --file
DMI.txt --overwrite
```

In-Band:

```
[SUM_HOME]# ./sum -c GetDmiInfo --file DMI.txt --overwrite
```

5.3.9 Editing DMI Information

There are two ways to edit DMI information for the managed system. You can either execute the EditDmiInfo command or manually edit the received DMI.txt file.

Manually Editing

1. Follow the steps in *5.3.8 Receiving DMI Information* to receive the DMI information text file (DMI.txt).
2. Replace the item values in the DMI.txt file with the desired values illustrated in *4.5 Format of DMI Information Text File*.
3. Remove the unchanged items in the text file. Note that this step is optional.

Note: The supported editable DMI items may be changed for different BIOS versions. The version variable of the DMI.txt file must be the same as that from the managed system and should not be edited.

Executing the EditDmiInfo Command

The EditDmiInfo command will only update (or add) the specified DMI item in the specified DMI.txt file. When you edit from an empty file, a new file will be created. You can specify a DMI item using [--item_type, --item_name] options or using --shn option with the item's short name. The editable item type, item name and item short name can be found in the DMI.txt file. To receive a DMI.txt file, follow the steps in *5.3.8 Receiving DMI Information*.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c EditDmiInfo --file
<DMI.txt> --item_type <Item Type> --item_name <Item Name> --value <Item Value>

sum [-i <IP or host name> -u <username> -p <password>] -c EditDmiInfo --file
<DMI.txt> --shn <Item Short Name> --value <Item Value>

sum [-i <IP or host name> -u <username> -p <password>] -c EditDmiInfo --file
<DMI.txt> --shn <Item Short Name> --default
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --item_type "System" --item_name "Version" --value "1.02"

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --shn SYVS --value "1.02"

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --shn SYVS --default
```

In-Band:

```
[SUM_HOME]# ./sum -c EditDmiInfo --file DMI.txt --shn SYVS --value 1.01
```

5.3.10 Updating DMI Information

1. Follow the steps in *5.3.9 Editing DMI Information* to prepare the edited DMI.txt file for updating DMI information.
2. Use the command ChangeDmiInfo with the edited DMI.txt file to run SUM to update the DMI information.

Notes:

- The supported editable DMI items may be changed for different BIOS versions. The version variable of the DMI.txt file must be the same as that from the managed system and should not be edited.
- The uploaded information will only take effect after a system reboots or powers up.
- X9DRL-3F/-iF MB does not support DMI related functions.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ChangeDmiInfo --file
<DMI.txt>  [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeDmiInfo --file
DMI.txt --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c ChangeDmiInfo --file DMI.txt --reboot
```

5.3.11 Setting Up BIOS Action

Use the command “SetBiosAction” to execute SUM to show or hide the settings related to BBS priority.

Note: The uploaded configurations will take effect only after the system is rebooted or powered up.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetBiosAction --BBS
<yes/no> [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBiosAction --BBS
yes --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c SetBiosAction --BBS no --reboot
```

5.3.12 Setting Up a BIOS Administrator Password

Use the command “SetBiosPassword” to execute SUM to update BIOS Administrator password.

Note: The uploaded new password will take effect only after the system is rebooted or powered up.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetBiosPassword
[[--new_password <new password> --confirm_password <confirm password>] | [--
pw_file <password file path>]] [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBiosPassword
--new_password 123456 --confirm_password 123456 --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBiosPassword
--pw_file passwd.txt --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c SetBiosPassword --new_password 123456 --confirm_password
123456 --reboot

[SUM_HOME]# ./sum -c SetBiosPassword --pw_file passwd.txt --reboot

passwd.txt:

    BiosPassword
```

5.3.13 Erasing the BIOS OA Key

Use the command “EraseOAKey” to execute SUM to erase the BIOS OA key.

Notes:

- The OA keys will be erased only after the system is rebooted or powered up.
- OOB and multi-OOB usages are only supported on X12/H12 and later platforms if BMC supports.

Syntax:

```
sum -c EraseOAKey [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c EraseOAKey
```

In-Band:

```
 [SUM_HOME]# ./sum -c EraseOAKey --reboot
```

5.3.14 Managing BIOS RoT Functions

The command BiosRotManage supports the following features on RoT systems of X12 and later platforms:

- **Getting Information on BIOS**

  Use the command BiosRotManage with the option "--action GetInfo" to retrieve information on active BIOS, backed-up BIOS and Golden BIOS.

- **Updating the Golden BIOS Image**

  Use the command BiosRotManage with the option "--action UpdateGolden" to replace the Golden image with an active BIOS image.

- **Recovering BIOS**

  Use the command BiosRotManage with the option "--action Recover" to recover BIOS from the backup image or the Golden image. By priority, the managed system recovers BIOS from the backup image. If the backup image is corrupted, it will then try to recover from the Golden image.

Notes:

- To execute the commands "UpdateGolden" or "Recover," it is necessary to power off a system, and requires the option --reboot.
- Use the "GetMaintenEventLog" command to check the results after the system is powered on. For details, see *5.5.3 Getting System Maintenance Event Log*.
- To execute the command "Recover," the SFT-DCMS-SINGLE license is required.
- This command is supported by OOB use and in-band usage is retricted to the Redfish host interface only.

Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
BiosRotManage --action <action> [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c BiosRotManage --
action UpdateGolden --reboot
```

The console output contains the following information.

```
.....
Note: System will be powered off shortly to continue the process. Please wait
for thesystem to power on again, then check the Maintenance Event log for
results.
Warning: Please wait for the system to power on again. Do not remove AC power
before the system reboots.
.................................................
.................................................
.................................................
.............
```

In-Band:

```
[SUM_HOME]# ./sum –I Redfish_HI –u ADMIN -p PASSWORD -c BiosRotManage --action
GetInfo
```

The console output contains the following information.

```
Managed system...........169.254.3.254
    BIOS build date.............2020/06/08
    Backup BIOS build date.........2020/05/05
    Golden BIOS build date.........2020/06/08
```

5.4 BMC Management for a Single System

5.4.1 Getting BMC Firmware Image Information

Use the command "GetBmcInfo" to receive the BMC firmware image information from the managed system as well as the BMC firmware image.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetBmcInfo [--file
<filename> [--file_only]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBmcInfo --file
SMCI_BMC.rom
```

In-Band:

```
[SUM_HOME]# ./sum -c GetBmcInfo --file SMCI_BMC.rom
```

The console output contains the following information when the local BMC image is non-RoT signed.

```
Managed system.....192.168.34.56
    BMC type.....X11_ATEN_AST2500_2
    BMC version.....12.63.00
    BMC ext. version.....01 00 00
Local BMC image file.....SMCI_BMC.rom
    BMC type.....X11_ATEN_AST2500_2
    BMC version.....12.63.00
    FW image.....Signed
        Signed Key.....NonRoT
[SUM_HOME]# ./sum -c GetBmcInfo --file SMCI_ROT_BMC.rom --file_only
```

The console output contains the following information when the local BMC image is RoT signed.

```
Local BMC image file......SMCI_ROT_BMC.rom
    BMC UFFN..............BMC_X12AST2600-ROT-5201MS_20210317_01.00.00_STDsp.bin
    BMC type..............X12_RoT_ATEN_AST2600
    BMC version...........01.00.00
    FW image..............Signed
        Signed Key........RoT
```

Non-RoT signed key of a local BMC image displays the following information:

Type	Description
Signed	The key is signed by Super Micro Computer, Inc.
Signed(U)	The key is NOT signed by Super Micro Computer, Inc., but by an unknown authority.
Verification failed	The signed information in the image cannot be verified, because the image is corrupted or incomplete.
(Not shown)	The “FW image” field is not shown because of no signed information in the image.

RoT-signed key of a local BMC image displays the following information:

Type	Description
Signed	RoT is signed by Super Micro Computer, Inc.
Signed(C)	RoT is verified by the specified certificate.
Signed(U)	RoT is NOT signed by Super Micro Computer, Inc. but by an unknown authority.
Verification failed	The RoT signing in the image cannot be verified because the image is corrupted or incomplete.

Note: For the platforms after X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, the BMC version supports 3 digits version.

5.4.2 Updating the BMC Firmware Image

Use the command “UpdateBmc” with BMC firmware image SMCI_BMC.rom to run SUM to update the managed system.

Notes:

- BMC will be reset after updating.
- BMC configurations will be preserved by default after updating unless --overwrite_cfg option is used.
- DO NOT flash BIOS and BMC firmware images at the same time.
- “UpdateBmc” command does not support AMI BMC FW. For OOB “UpdateBmc” usage, please use SUM version 1.4.2.
- --overwrite_cfg option overwrites the current BMC configuration using the factory default values in the given BMC image file.
- --overwrite_sdr option overwrites current BMC SDR data. For AMI BMC FW, it is also required to use the --overwrite_cfg option.
- Signed BMC update is supported.
- For X12/H12 and later platforms except H12 non-RoT systems, in-band update BMC can only be done through Redfish Host Interface. For detail, refer to *4.10 Redfish Host Interface*.
- The --backup option backs up the current BMC image on the managed system, not the BMC file updated to the managed system.
- The --backup option only supported by the X12/H12 and later RoT platforms.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--
forward] [--overwrite_ssl]
```

Example:

OOB :

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBmc --file
SMCI_BMC.rom
```

In-Band:

```
[SUM_HOME]# ./sum -c UpdateBmc --file SMCI_BMC.rom

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateBmc --file
SMCI_BMC.rom
```

5.4.3 Receiving BMC Settings

Use the command "GetBmcCfg" to execute SUM to get the current BMC settings from the managed system and save it in the BMCCfg.xml file.hey

Notes:

- Received tables/elements might not be identical between two managed systems. Only supported tables/elements for the managed system will be received.
- For in-band and OOB usages, note that the file formats for receiving BMC settings may be different. Be careful not to misuse them.
- SUM gets/changes syslog table in BMC configuration through HTTPS so that syslog information in BMC conguration will be lost if HTTPS is disabled..
- For OOB operation, if BMC supports the account lockout configuration, the <Account> table will replace the <UserManagement> table.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetBmcCfg --file
<BMCCfg.xml> [--overwrite]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBmcCfg --file
BMCCfg.xml --overwrite
```

In-Band:

```
[SUM_HOME]# ./sum -c GetBmcCfg --file BMCCfg.xml --overwrite
```

5.4.4 Updating BMC Settings

1. Follow the steps in *5.4.3 Receiving BMC settings*.

2. Edit the configurable element values in the BMC configuration text file BMCCfg.xml to the desired values as illustrated in *4.6 Format of BMC Configuration Text File*.
3. Skip unchanged tables in the text file by setting the Action attribute as "None". Note that this step is optional.
4. Remove unchanged tables/elements in the text file. Note that this step is optional.
5. Use the command ChangeBmcCfg with the updated BMCCfg.xml file to run SUM to update the BMC configuration.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ChangeBmcCfg --file
<BMCCfg.xml>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeBmcCfg --file
BMCCfg.xml
```

In-Band:

```
[SUM_HOME]# ./sum -c ChangeBmcCfg --file BMCCfg.xml
```

Notes: Pay attention to the following notes when modifying contents inside the XML element <LAN>.

- The connection could be broken if the LAN configuration is changed.
- For in-band operation, all data of the element <Configurations> inside the element <LAN> is configurable.
- For OOB operation, if Redfish is not supported, all configurations inside the element <LAN> are read only.
- For OOB operation, the configurations of the element <DynamicIPv6> and the element <StaticIPv6> are read only.
- For OOB operation, if BMC supports the account lockout configuration, the <Account> table will replace the <UserManagement> table.

5.4.5 Installing BMC Certification

To enhance security, SUM supports identity certification, which allows a user to upload a certification file to the BMC. The example below shows how a certificate file and key should be set up in the BMC configuration file.

```
<Certification Action="Change">
    <!--Supported Action:None/Change-->
    <Information>
      <CertStartDate>Jul 27 00:00:00 2018 GMT</CertStartDate>
      <CertEndDate>Jul 27 00:00:00 2021 GMT</CertEndDate>
    </Information>
    <Configuration>
      <!--Configurations for BMC certifications-->
      <CertFile>/home/test/cert.pem</CertFile>
      <!--string value; path to file-->
      <PrivKeyFile>/home/test/key.pem</PrivKeyFile>
      <!--string value; path to file-->
      <!--BMC will be reset after uploading this file-->
    </Configuration>
  </Certification>
```

- To set the value in <CertFile></CertFile>
  a file path(/home/test/) follow by a filename(cert.pem)
- To set the value in < PrivKeyFile ></ PrivKeyFile >
  a file path(/home/test/) follow by a filename(key.pem)

5.4.6 Setting Up a BMC User Password

Use the command “SetBmcPassword” to execute SUM to update BMC user password.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetBmcPassword
[--user_id <user ID>] [[--new_password <new password> --confirm_password
<confirm password>] | [--pw_file <password file path>]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcPassword
--user_id 3 --new_password 12345678 --confirm_password 12345678

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcPassword
--pw_file passwd.txt
```

In-Band:

```
[SUM_HOME]# ./sum -c SetBmcPassword --new_password 12345678 --confirm_password
12345678

[SUM_HOME]# ./sum -c SetBmcPassword --user_id 3 --pw_file passwd.txt

passwd.txt:

    BmcPasswordString
```

Note: Without the option --user_id, the user ID is set to 2 (as Administrator) by default.

5.4.7 Receiving the BMC KCS Privilege Level

Use the command "GetKcsPriv" to execute SUM to get the current BMC KCS privilege level from the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetKcsPriv
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetKcsPriv
```

In-Band:

```
[SUM_HOME]# ./sum -c GetKcsPriv
```

The console output contains the following information.

```
Managed system.................192.168.34.56

    KCS Privilege Level.......4 (Administrator)
```

5.4.8 Setting the BMC KCS Privilege Level

Use the command "SetKcsPriv" to execute SUM to set the BMC KCS privilege level.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetKcsPriv --
priv_level <KCS privilege level>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetKcsPriv
--priv_level 'Call Back'

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetKcsPriv
--priv_level 1
```

Notes:

- SUM only supports the following KCS privileges: Call Back, User, Operator and Administrator.
- This command only supports OOB usage.
- The BMC KCS privilege can be set through a numberic ID or a name.

5.4.9 Loading Factory BMC Settings

Since November 2019, Supermicro has implemented a new security feature for the BMC firmware stack on all new X10, X11, X12 H11, H12, and **all future generation Supermicro products**. Supermicro will no longer use the default password "ADMIN" for new devices or systems. All such systems are shipped with a "Unique Pre-Programmed Password" for user admin on every hardware device with BMC.

For more information about the implementation of a BMC unique password and how to locate it, please refer to the BMC Unique Password Guide.

Use the command LoadDefaultBmcCfg to execute SUM to reset the BMC of the managed system to the factory default. Allowed option combinations depend on the managed system state. Unsupported option combinations will be denied.

	Reset Network	**Reset Users info**	**Reset FRU**	**ADMIN Password**
Option: --preserve_user_cfg	N	N	N	Preserved
Option: --clear_user_cfg with --load_default_password	N	Y	N	ADMIN
Option: --clear_user_cfg with --load_unique_password	N	Y	N	Unique Password

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c LoadDefaultBmcCfg --
preserve_user_cfg
```

```
sum [-i <IP or host name> -u <username> -p <password>] -c LoadDefaultBmcCfg --
clear_user_cfg --load_unique_password

sum [-i <IP or host name> -u <username> -p <password>] -c LoadDefaultBmcCfg --
clear_user_cfg --load_default_password
```

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg --
preserve_user_cfg

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg --
clear_user_cfg --load_unique_password

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg --
clear_user_cfg --load_default_password
```

In-Band:

```
[SUM_HOME]# ./sum -c LoadDefaultBmcCfg --preserve_user_cfg [--reboot]

[SUM_HOME]# ./sum -c LoadDefaultBmcCfg --clear_user_cfg --load_unique_password
[--reboot]

[SUM_HOME]# ./sum -c LoadDefaultBmcCfg --clear_user_cfg --load_default_password
[--reboot]
```

Notes:

- The option --load_unique_password only supports systems installed with a BMC unique password.
- This command will not reset any network settings.

5.4.10 Acquiring the BMC System Lockdown Mode

When the System Lockdown Mode is enabled on a managed system, neither setting configurations nor updating firmware is not allowed in this mode. To learn about the managed system status, use the command “GetLockdownMode”.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetLockdownMode
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetLockdownMode
```

The console output contains the following information.

```
Managed system.............192.168.34.56

    System Lockdown..........No
```

In-Band:

```
[SUM_HOME]# ./sum -c GetLockdownMode
```

The console output contains the following information.

```
Managed system.............localhost

    System Lockdown..........No
```

5.4.11 Setting the BMC System in Lockdown Mode

Use the command "SetLockdownMode" to execute SUM to set the BMC system in Lockdown Mode.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetLockdownMode --lock
<yes/no> --reboot
```

Example:

```
OOB:

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetLockdownMode
--lock <yes/no> --reboot
```

5.4.12 Managing BMC RoT Functions

The command "BmcRotManage" supports the following features on RoT systems of X12 and later platforms:

- **Getting Information on BMC**

  Use the command BmcRotManage with the option "--action GetInfo" to retrieve information on active BMC, backed-up BMC and Golden BMC.

- **Updating the Golden Image**

  Use the command BmcRotManage with the option "--action UpdateGolden" to replace the Golden image with an active BMC firmware.

- **Recovering BMC**

  Use the command BmcRotManage with the option "--action Recover" to recover BMC from the backup image or the Golden image. By priority, the managed system recovers BMC from the backup image. If the backup image is corrupted, it will then recover from the Golden image.

Notes:

- BMC will be disconnected while updating the Golden image and recovering the firmware. Use the command "GetMaintenEventLog" to check the result afterwards. For details, see *5.5.3 Getting System Maintenance Event Log*.

- The SFT-DCMS-SINGLE license is required to recover BIOS.
- This command is only available for OOB and in-band usages retricted to Redfish host interface.

Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
BmcRotManage --action <action>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c BmcRotManage --action
GetInfo
```

The console output contains the following information.

```
Managed system.....................192.168.34.56
    BMC version.....................09.10.19
    Backup BMC version.............00.10.08
    Golden BMC version.............09.10.19
```

In-Band:

```
[SUM_HOME]# ./sum –I Redfish_HI –u ADMIN -p PASSWORD -c BmcRotManage --action
UpdateGolden
```

The console output contains the following information.

```
..........
Status: System is backing up current FW as golden image and BMC will be offline
for 6 minutes.
.....................................
.....................................
Done
Status: Please check Maintenance Event log for result.
```

5.4.13 Setting the BMC Reset Counter

To set the BMC reset counter, use the command “TimedBmcReset”.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c TimedBmcReset --delay
<BMC reset delay time>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TimedBmcReset --delay
10
```

The console output contains the following information.

```
The BMC will be reset after 10 minute.
```

In-Band:

```
[SUM_HOME]# ./sum -c TimeBmcReset --delay 20
```

The console output contains the following information.

```
The BMC will be reset 20 minutes later.
```

- **Note:** This command is not available on X12 and H12 RoT platforms.

5.5 Event Log Management for a Single System

5.5.1 Getting System Event Log

Use the command “GetEventLog” to execute SUM to show the current system event log (including both BIOS and BMC event log) from the managed system. With the --file option, the event log can be saved in the EventLog.txt file.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetEventLog [--file
<EventLog.txt>] [--overwrite]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetEventLog --file
EventLog.txt --overwrite
```

In-band:

```
[SUM_HOME]# ./sum -c GetEventLog --file EventLog.txt --overwrite
```

5.5.2 Clearing System Event Log

Use the command “ClearEventLog” to execute SUM to clear the event log (both BMC and BIOS event log) in the managed system.

Notes:

- Both BIOS and BMC event log in BMC will be cleared immediately.
- BIOS event log in BIOS will be cleared only after system reboot.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ClearEventLog [--
reboot] [--clear_bmc_eventlog] [--clear_bios_eventlog]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ClearEventLog --
reboot
```

In-band:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ClearEventLog --
reboot
```

5.5.3 Getting System Maintenance Event Log

Use the "GetMaintenEventLog" command to have SUM show the managed system's current maintenance event logs (including both BIOS and BMC maintenance event logs). Both options --st and --et are required to show logs at the specified time. With the option "--count," the command GetMaintenEventLog can show the specified number of logs. With the option "--file," the maintenance event log can be saved in a MaintenEventLog.txt file.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetMaintenEventLog --
st <start time> --et <end time> [--count <log count>] [--file <EventLog.txt>] [-
-overwrite]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetMaintenEventLog --
st 20200601 --et 20200608 --count 10 --file MaintenEventLog.txt --overwrite
```

In-band:

```
[SUM_HOME]# ./sum -c GetMaintenEventLog --st 20200510 --et 20200610 --count 20 -
--file MaintenEventLog.txt --overwrite
```

5.5.4 Getting Host Crash Dump Log

Use the "GetHostDump" command to have SUM show the managed system's crash dump file. This function is only available on H12 RoT and X12 2600 and later platforms.

- **Creating and downloading the host crash dump data**

  Use the command GetHostDump with the option "--action CreateDump" to create the managed system's crash dump file and download it from BMC.

- **Deleting the host crash dump data on BMC**

  Use the command GetHostDump with the option "--action DeleteDump" to delete a crash dump file on BMC.

- **Directly downloading the host crash dump data from BMC**

  Use the command GetHostDump with the option "--action DirectDump" to download the managed system's crash dump file from BMC. If the crash dump file does not exist, SUM will show the warning message "No dump messages exist, please create a dump message first".

Notes:

- The downloaded file is a compressed file, and save it in .tgz format.
- The option "--file" is required for both options "--action CreateDump" and "--action DirectDump".
- The option "--action CreateDump" is not available on H12 RoT platforms.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c GetHostDump --action
<actiondump> [--file <HostDump.tgz>] [--overwrite]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetHostDump --action
CreateDump --file HostDump.tgz --overwrite
```

5.5.5 Clearing System Maintenance Event Log

Use the “ClearMaintenEventLog” command to execute SUM to clear the maintenance event log in the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ClearMaintenEventLog
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ClearMaintenEventLog
```

In-band:

```
[SUM_HOME]# ./sum -c ClearMaintenEventLog
```

5.6 CMM Management for a Single System (OOB Only)

The CMM provides total remote control of individual blade server nodes, power supplies, power fans, and networking switches. The controller is a separate processor, allowing all monitoring and control functions to operate flawlessly regardless of CPU operation or system power-on status.

Note: Three models of 7U SuperBlade CMMs, including SBM-CMM-001, BMB-CMM-002 (mini-CMM) and SBM-CMM-003 are no longer supported.

5.6.1 Receiving CMM Firmware Image Information

Use the command "GetCmmInfo" to receive the CMM firmware image information from the managed system as well as the CMM firmware image.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetCmmInfo [--file
<filename> [--file_only]]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCmmInfo --file
SMCI_CMM.rom
```

The console output contains the following information.

```
Managed system..........192.168.34.56
    CMM type............MicroCMM
    CMM version.........09.01
Local CMM image file.....SMCI_CMM.rom
    CMM type............MicroCMM
    CMM version.........09.10
```

5.6.2 Updating the CMM Firmware Image

Use the command “UpdateCmm” with the CMM firmware image SMCI_CMM.rom to update the managed system.

Notes:

- CMM will be reset after updating.
- CMM configurations will be preserved after updating unless the --overwrite_cfg option is used.
- DO NOT flash BIOS and BMC firmware images at the same time.
- For OOB UpdateCmm usage, please use SUM version 1.6.2 or later.
- The --overwrite_cfg option overwrites the current CMM configurations, including network settings using factory default values in the given CMM firmware image. This might cause the IPMI connection to be lost.
- The --overwrite_sdr option overwrites the current CMM SDR data. Currently this option is only supported by the JBOD CMM system “CSE-947HE2C-R2K05JBOD”. Other CMM system with this option won’t take effect.
- The --overwrite_ssl option overwrites the current CMM SSL configuration. Currently this option is only supported by the JBOD CMM system “CSE-947HE2C-R2K05JBOD”. Other CMM systems with this option won’t take effect.
- If the CMM FW web server becomes unreachable after CMM FW is updated, use the ipmitool to troubleshoot. Follow these steps:
  a. Reset CMM.
     $ ipmitool -H ${CMM_IP} -U {CMM_USER} -P {CMM_PASSWD} raw 0x30 0x34 0x05
  b. Wait for 3 minutes and then check if the CMM web is reachable. If it is reachable, the troubleshooting is done.
  c. If the CMM web is still unreachable, load the CMM factory defaults.
     (**Note:** All CMM settings except LAN/FRU will be LOST.)
     $ ipmitool -H ${CMM_IP} -U {CMM_USER} -P {CMM_PASSWD} raw 0x30 0x33 0x14
  d. Wait for 3 minutes and check the CMM web again.
- To update the JBOD system “CSE-946ED-R2KJBOD” and “CSE-947HE2C-R2K05JBOD,” use the command UpdateCmm.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c UpdateCmm --file
<filename> [--overwrite_cfg] [--overwrite_sdr] [--overwrite_ssl]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateCmm --file
SMCI_CMM.rom
```

5.6.3 Receiving CMM Settings

Use the command “GetCmmCfg” to execute SUM to get the current CMM settings from the managed system and save them in the CMMCfg.xml file.

Note: Received tables/elements might not be identical between two managed systems. Only tables/elements supported for the managed system will be received.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetCmmCfg --file
<CMMCfg.xml> [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCmmCfg --file
CMMCfg.xml --overwrite
```

5.6.4 Updating CMM Settings

1. Follow the steps in *5.6.3 Receiving CMM settings*.
2. Edit the configurable element values in the CMM configuration file CMMCfg.xml to the desired values as illustrated in *4.8 CMM Configuration Text File Format*.
3. Set the Action attribute as "None" to skip the unchanged tables in the text file. Note that this step is optional.
4. Remove unchanged tables/elements in the text file. Note that this step is optional.
5. Use the command ChangeCmmCfg with the updated CMMCfg.xml file to run SUM to update the CMM configuration.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ChangeCmmCfg --file
<CMMCfg.xml>
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeCmmCfg --file
CMMCfg.xml
```

Note: The connection might be lost if the LAN configuration is changed.

5.6.5 Setting Up a CMM User Password

Use the command “SetCmmPassword” to execute SUM to update the CMM user password..

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetCmmPassword
[--user_id <user ID>] [[--new_password <new password> --confirm_password
<confirm password>] | [--pw_file <password file path>]]
```

Example:

```
OOB:

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmPassword
--user_id 3 --new_password 12345678 --confirm_password 12345678

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmPassword
--pw_file passwd.txt

In-Band:

[SUM_HOME]# ./sum -c SetCmmPassword --new_password 12345678 --confirm_password
12345678

[SUM_HOME]# ./sum -c SetCmmPassword --user_id 3 --pw_file passwd.txt

passwd.txt:

    CmmPasswordString
```

Note: Without the option --user_id, the user ID is set to 2 (as Administrator) by default.

5.6.6 Loading Factory CMM Settings

Use the command "LoadDefaultCmmCfg" to have SUM reset the CMM settings of the managed system to the factory defaults. Allowed option combinations depend on the managed system state. The unsupported options will be denied. For more detailed information of unique passwords, see *5.4.9 Loading Factory BMC Settings*.

Option	Reset Network	Reset Users info	Reset FRU	ADMIN Password
--preserve_user_cfg	N	N	N	Preserved
--clear_user_cfg with --load_default_password	N	Y	N	ADMIN
--clear_user_cfg with --load_unique_password	N	Y	N	Unique Password

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c LoadDefaultCmmCfg --preserve_user_cfg
```

```
sum -i <IP or host name> -u <username> -p <password> -c LoadDefaultCmmCfg --clear_user_cfg --load_unique_password
```

```
sum -i <IP or host name> -u <username> -p <password> -c LoadDefaultCmmCfg --clear_user_cfg --load_default_password
```

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c LoadDefaultCmmCfg --preserve_user_cfg
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c LoadDefaultCmmCfg --clear_user_cfg --load_unique_password
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c LoadDefaultCmmCfg --
clear_user_cfg --load_default_password
```

Notes:

- The option --load_unique_password only supports systems installed with a CMM unique password.
- This command will not reset any network settings.

5.6.7 Receiving BBP Firmware Image Information

Use the command "GetBbpInfo" to receive the BBP firmware image and its information from the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetBbpInfo [--file
<filename> [--file_only]]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBbpInfo --file
BBP.bin
```

The console output contains the following information.

```
Managed system...........172.30.143.96
    BBP version.........01.08
Local BBP image file.....BBP_EC_2019-03-14_1901.47v1.08.bin
    BBP version.........01.08
```

5.6.8 Updating the BBP Firmware Image

Use the command “UpdateBbp” with the BBP firmware image BBP.bin to update the BBP of managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c UpdateBbp --file
<filename> [--skip_check]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBbp --file
BBP.rom
```

Note: It is recommended all system units be turned off by the CmmPowerStatus command. If you need to update BBP while system units are powered on, please make sure that enough power is being provided, and then use the option --skip_check to force BBP to update. If the power is insufficient while updating BBP, the blade system may shut down.

5.6.9 Getting Current Power Status of Blade System

Use the command “GetBladePowerStatus” to get the current power status of the blade system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetBladePowerStatus
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBladePowerStatus
```

The console output contains the following information:

```
 Blade       | Node     | Power
-------------|----------|----------
 Blade  A1   | Node  1  | On
 Blade  A2   | Node  1  | On
 Blade  A3   | Node  1  | On
 Blade  A4   | Node  1  | On
 Blade  A5   | Node  1  | On
 Blade  A6   | Node  1  | On
 Blade  A7   | Node  1  | On
 Blade  A8   | Node  1  | On
 Blade  A9   | Node  1  | On
 Blade  A10  | Node  1  | On
```

5.6.10 Setting Power Status of Blade System

SUM supports blade power status management. You can apply power action to the whole blade system, a single blade, or a node through the specified option. For example, to apply power action to the whole blade system, you only need to assign a power action. To apply a power action to the specified single blade system, you must assign a power action and the option --blade with index. To apply power action to a specified node of a blade system, you must assign a power action and the options --blade and --node with index.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetBladePowerAction --action <action> --blade <Blade Index> [--node <Node Index>]
```

Option Commands	Descriptions
--action	Sets power action with: 0 = down 1 = up 2 = cycle 3 = reset 4 = accycle 5 = softshutdown
--blade	Assigns blade index. [A1-A14], [B1-B14] or "ALL"
--node (optional)	Assigns node index. [1-4]

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBladePowerAction --action down --blade ALL
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBladePowerAction
--blade A1 --action reset

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBladePowerAction
--blade A1 --node 1 --action softshutdown
```

5.7 Applications for a Single System

5.7.1 Providing an ISO Image as a Virtual Media through BMC and File Server

Use the command "MountIsoImage" to mount ISO image as a virtual media to the managed system through SAMBA/HTTP server. Since SUM 2.5.0, SUM has a new rule of using new special charaters for virtual media. For more details, see the tables below.

HTTP URL format:

HTTP URL	http://<hostname or IP>/<shared point>/<file path> http://<hostname or IP>:<port number>/<shared point>/<file path>
Share host	http://<hostname or IP> http://<hostname or IP>:<port number>
Path to image	<shared point>/<file path>

SAMBA URL/UNC format:

SAMBA URL	smb://<hostname or IP>/<shared point>/<file path> smb://<hostname or IP>:<port number>/<shared point>/<file path>
SAMBA UNC	\\<hostname or IP>\<shared point>\<file path> \\<hostname or IP>:<port number>\<shared point>\<file path>
Share host	<hostname or IP> or <hostname or IP>:<port number>
Path to image	<shared point>/<file path>

Allowed character classes:

- a-z
- A-Z
- 0-9
- Special characters for ID and password: ^ (a caret).
- Special characters for a shared host: - (a dash).

- Special character for a shared host in HTTP and SAMBA protocols in an IPv6 URL: : (a colon)
- The shared host for HTTP IPv6 address should be enclosed by square brackets: [ ]
- Special characters for path to image: @,^,-,_,., /, and \ (Note that a slash/ and a backslash \ can only be used in a path.)
- Special characters like backslashes \ and slashes / should only be used once; repeated use (e.g., //, \\, /\ and \/) are not allowed.
- Special character ^ (a caret) is not available for use in older versions of BMC firmware.
- The port number may not be supported in older versions of BMC firmware.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c MountIsoImage --
image_url <URL> [[--id <id for URL> --pw <password for URL>] | [--id <id for
URL> --pw_file <password file path>]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MountIsoImage  --
image_url 'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MountIsoImage  --
image_url 'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MountIsoImage  --
image_url 'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MountIsoImage  --
image_url 'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbid
--pw_file smbpasswd.txt
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MountIsoImage  --
image_url '\\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id smbid --pw_file
smbpasswd.txt

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MountIsoImage  --
image_url '\\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id smbid --pw_file
smbpasswd.txt

smbpasswd.txt:
smbpasswd
```

In-band:

```
[SUM_HOME]# ./sum -c MountIsoImage  --image_url
'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -c MountIsoImage  --image_url
'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -c MountIsoImage  --image_url
'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -c MountIsoImage  --image_url
'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd

[SUM_HOME]# ./sum -c MountIsoImage  --image_url
'\\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id smbid --pw_file
smbpasswd.txt

[SUM_HOME]# ./sum -c MountIsoImage  --image_url
'\\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id smbid --pw_file
smbpasswd.txt

smbpasswd.txt:
smbpasswd
```

Notes:

- Special characters for ID and password: ^ (a caret).
- Special characters for shared host: - (a dash).
- Special character for HTTP and SAMBA protocols in an IPv6-format URL shared host: : (a colon).
- Share host for HTTP protocol in IPv6 format must be enclosed with square brackets ([ ])
- Special characters for path to image: @^-_./\ (/ and \ can only be used in a path)
- Special characters like backslashes \ and slashes / should only be used once; repeated use (e.g., //, \\, /\ and \/) is not allowed.
- Special character ^ is not available for use in older versions of BMC firmware.
- The port number may not be supported in older versions of BMC firmware.

5.7.2 Removing ISO Image as a Virtual Media

Use the command “UnmountIsoImage” to remove ISO image as a virtual media from the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c UnmountIsoImage
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UnmountIsoImage
```

In-Band:

```
[SUM_HOME]# ./sum -c UnmountIsoImage
```

5.7.3 Mounting a Floppy Image as a Virtual Media from a Local Image File

Use the command "MountFloppyImage" to have SUM mount a binary floppy image to the managed system virtually.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c MountFloppyImage

--file <filename>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MountFloppyImage --
file Floppy.img
```

In-band:

```
[SUM_HOME]# ./sum -c MountFloppyImage --file Floppy.img
```

The console output will be as below.

```
Supermicro Update Manager (for UEFI BIOS) 2.5.0 (2020/02/07) (x86_64)

Copyright(C) 2013-2020 Super Micro Computer, Inc. All rights reserved.

Status: Checking node product key...

Status: The floppy image file "Floppy.img" is mounting...

.................

Status: The floppy image file "Floppy.img" is mounted successfully.
```

Note: A floppy image size should be 1.44MB.

5.7.4 Unmounting a Floppy Image as Virtual Media from the Managed System

Use the command “UnmountFloppyImage” to execute SUM to remove a binary floppy image from the managed system virtually.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c UnmountFloppyImage
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UnmountFloppyImage
```

In-band:

```
[SUM_HOME]# ./sum -c UnmountFloppyImage
```

The console output will be as below.

```
Supermicro Update Manager (for UEFI BIOS) 2.5.0 (2020/02/07) (x86_64)

Copyright(C) 2013-2020 Super Micro Computer, Inc. All rights reserved.

Status: Checking node product key...

Status: The floppy image file is unmounting...
```

Status: The floppy image file is unmounted successfully.

5.7.5 Sending an IPMI Raw Command

Use the command “RawCommand” to send an IPMI raw command to the target system

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c RawCommand --raw  <raw command>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c RawCommand --raw '06 01'

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c RawCommand --raw '0x06 0x01'
```

In-band:

```
[SUM_HOME]# ./sum -c RawCommand --raw '06 01'

[SUM_HOME]# ./sum -c RawCommand --raw '0x06 0x01'
```

The console output contains the following information.

```
00
20 01 09 95 02 BF 7C 2A 00 7A 09 00 10 00 00
```

Note: A raw command has to be in double quotation marks.

5.7.6 USB Port Accessibility Control

In order to prevent security data from being leaked and unauthorized operations through USB ports, since X12, SUM has supported inband USB port accessibility control for front and rear panels. Currently, SUM does not support USB port accessibility control for AMD platforms. Front panel means the USB ports are connected to a 19-pin USB header on motherboard and usually is accessible in front of a system. In constrast, rear panel means the built-in USB ports on motherboard and usually is accessible in the rear of a system. For formal USB port position definition, please refer to "_PLD" (Physical Location of Device) in ACPI specifiation. USB port accessibility can be configured by BIOS configuration during POST. BIOS settings "Front USB Port(s)" and "Rear USB Port(s)" are for front and rear panels, respectively.

Three options are provided:

- **Enabled:** A USB port is statically enabled or disabled by BIOS during POST, and it can't be dynamically enabled or disabled in the running operating system.
- **Disabled:** A USB port is statically enabled or disabled by BIOS during POST.
- **Enabled (Dynamically):** A USB port access mode can be dynamically switched and taken effect immediately in the running operating system.

The USB port accessibility in the running operating system can be accessed by running the command "GetUsbAccessMode" (see *5.7.7 Receiving USB Port Access Mode (Inband only)*), or switched by running the command "SetUsbAccessMode" (see *5.7.8 Dynamic Control USB Port Access Mode (Inband only)*). The mapping releatationship between BIOS setting options and access mode(s) in the running operating system are summarized in the following table.

BIOS Setting Options for USB Ports	Access Mode(s) in the Running Operating System	Dynamic Control in the Running Operating System
Enabled	Statically enabled	No
Disabled	Statically disabled	No
Enabled (Dynamically)	Dynamically enabled/disabled	Yes

5.7.7 Acquiring USB Port Access Mode (Inband Only)

Use the inband command "GetUsbAccessMode" to receive USB access mode in the running operating system. Currently, SUM supports for dynamically disabling/enabling both front and rear panel USB ports. There are four USB port access modes:

- **Dynamically Enabled:** A USB port is dynamically enabled.
- **Dynamically Disabled:** A USB port is dynamically disabled.
- **Statically Enabled:** A USB port is enabled by BIOS during POST, and it cannot be dynamically enabled in the running operating system.
- **Statically Disabled:** A USB port is disabled by BIOS during POST, and it cannot be dynamically enabled in the running operating system.

Syntax:

```
sum -c GetUsbAccessMode
```

Example:

In-Band:

```
[SUM_HOME]# ./sum -c GetUsbAccessMode
```

The console output contains the following information.

```
[USB access mode]

REAR panel.....................dynamic enabled

FRONT panel...................static disabled
```

5.7.8 Dynamically Controling USB Port Access Mode (Inband Only)

Only when “Front USB Port(s)” or “Rear USB Port(s)” is set to “Enabled (Dynamic)” in the BIOS configurations is the command “SetUsbAccessMode” allowed to dynamically enable/disable the USB port access mode.

Syntax:

```
sum -c SetUsbAccessMode --panel <front/rear> --disable

sum -c SetUsbAccessMode --panel <front/rear> --enable
```

Example:

In-Band:

```
[SUM_HOME]# ./sum -c setUsbAccessMode --panel front --disable
```

The console output contains the following information.

```
[USB access mode]

FRONT panel.....................dynamic disabled
```

Note: For some systems, a plugged-in USB 3.0 device cannot be used after the port is dynamically disabled and enabled again. When the device cannot be used after the port is dynamically enabled, SUM will output a message "USB 3.0 device may need to be manually unplugged and plugged for use" to bring this to the user’s attention.

5.7.9 Controlling the UID of the Managed System

The UID is a unit identifier button for easy system location in large stack configurations. Use the command "LocateServerUid" to control the UID. When the UID is enabled, the blue LED on both the front and rear of the chassis will be illuminated.

Option Commands	Descriptions
--action	Sets action to: 1 = GetStatus 2 = On 3 = Off

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c LocateServerUid –
action <action>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c LocateServerUid --
action 3
```

The console output contains the following information.

```
UID of the managed system is turned off.
```

In-Band:

```
[SUM_HOME]# ./sum -c LocateServerUid --action GetStatus
```

The console output contains the following information.

```
Managed system.................localhost

    UID status.................Off
```

5.7.10 Booting into the ISO image from HTTP Server

Use the command “SetHttpBoot” to download an ISO image from the HTTP server and boot into the ISO image.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetHttpBoot [--
boot_lan <boot lan port>] [--boot_name <boot description>] --image_url <URL> [--
reboot]

sum [-i <IP or host name> -u <username> -p <password>] -c SetHttpBoot --
boot_clean [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetHttpBoot --
boot_lan 1 --boot_name bootDescription --image_url
http://192.168.12.78/iso/boot.iso --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetHttpBoot --
boot_lan 2 --boot_name bootDescription --image_url
https://[1234:ab5:0:c678:9012:345d:6e78:9f0a]/iso/boot.iso --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetHttpBoot --
boot_clean --reboot
```

In-band:

```
[SUM_HOME]# ./sum SetHttpBoot --boot_lan 1 --boot_name bootDescription --
image_url http://192.168.12.78/iso/boot.iso --reboot

[SUM_HOME]# ./sum -c SetHttpBoot --boot_lan 2 --boot_name bootDescription --
image_url https://[1234:ab5:0:c678:9012:345d:6e78:9f0a]/iso/boot.iso --reboot

[SUM_HOME]# ./sum -c SetHttpBoot –boot_clean --reboot
```

Notes:

- HTTPS boot needs to provide the clients with a valid TLS certificate signed by a trusted Certificatio Authority. Please use the "ChangeBiosCfg" command to upload the TLS certificate, see *E.5.1 File Upload*.
- Due to BIOS limitations, if an HTTP boot option exists in the BIOS configuration, please use the option --boot_clean to clean the HTTP boot option and then reset HTTP the boot option.

5.8 Storage Management for a Single System

5.8.1 Getting RAID Firmware Image Information

Use the command "GetRaidControllerInfo" to receive the RAID firmware image information from the managed system or the RAID firmware image.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
GetRaidControllerInfo [--file <filename> [--file_only]] [--controller <Broadcom
or Marvell>] [--dev_id <controller_id>]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetRaidControllerInfo
--file RAID.rom
```

In-band:

```
[SUM_HOME]# ./sum -c GetRaidControllerInfo --file RAID.rom
```

The console output contains the following information.

```
Managed System.....................   192.168.34.56
Device ID..........................   Device 0
Product Name.......................   AVAGO 3108 MegaRAID
Serial.............................   N/A
Package............................   24.18.0-0021
Firmware Version...................   4.670.00-6500
BIOS Version.......................   6.34.01.0_4.19.08.00_0x06160200
Boot Block Version.................   3.07.00.00-0003
```

```
Local RAID Firmware Image File........   AVAGO_3108_4.680.00-8290.rom

Product Name..........................   AVAGO 3108 MegaRAID

Package...............................   24.21.0-0028

Firmware Version......................   4.680.00-8290

BIOS Version..........................   6.36.00.2_4.19.08.00_0x06180202

Boot Block Version....................   3.07.00.00-0003
```

Notes:

- For X11 platforms, the “GetRaidControllerInfo” command only supports Broadcom 3108.
- For X12 and later platforms, the “GetRaidControllerInfo” command only supports Broadcom 3008, 3108 and Marvell SE9230.

5.8.2 Updating the RAID Firmware Image

Use the command UpdateRaidController with RAID firmware image RAID.rom to update the managed system.

Notes:

- The "UpdateRaidController" command only supports Broadcom 3108 and Marvell SE9230.
- Broadom 3108 is supported by the following firmware images:
  - RAID firmware image of version 4.650.00-8095 and later
  - For X10 Intel® Xeon® Processor E5 v3/v4 Product Family platform, BMC firmware images of version REDFISH 3.52 and later
  - For X11 Intel® Xeon® Processor E3-1200 v5 Product Family platform, BMC firmware images of version ATEN X11 1.33 and later
  - For X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets platform, BMC firmware images of version ATEN X11DP 1.10 and later
  - Supported on X12 and later platforms.
- For Marvell SE9230:
  - Supported on X12 and later platforms.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
UpdateRaidController  --file <filename> --controller <Broadcom or Marvell> --
dev_id <RAID controller device ID> [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateRaidController
--controller Broadcom --dev_id 0 --file RAID.rom –reboot
```

In-band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateRaidController --
controller Marvell --dev_id 0 --file RAID.rom --reboot
```

5.8.3 Receiving RAID Settings

Use the command “GetRaidCfg” to execute SUM to get the current RAID settings from the managed system and save it in the RAIDCfg.xml file.

Notes:

- The received tables/elements between the two managed systems might not be identical. Only the supported tables/elements for the managed system will be received.
- The SUM cannot get or change the RAID configurations of JBOD mode setting under the Controller Properties in an in-band enviroment.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetRaidCfg --file
<RAIDCfg.xml> [--overwrite]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetRaidCfg --file
RAIDCfg.xml --overwrite
```

In-band:

```
[SUM_HOME]# ./sum -c GetRaidCfg --file RAIDCfg.xml --overwrite
```

5.8.4 Updating RAID Settings

1. Follow the steps in *5.8.3 Receiving RAID Settings*.
2. Edit the configurable element values in the RAID configuration text file RAIDCfg.xml as illustrated in *4.7 RAID Configuration XML File format*.
3. Set the Action attribute as "None" to skip the unchanged tables in the text file. Note that this step is optional.
4. Remove the unchanged tables/elements in the text file. Note that this step is optional.
5. Use the command "ChangeRaidCfg" with the updated RAIDCfg.xml file to run SUM to update the RAID configuration.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ChangeRaidCfg --file
<RAIDCfg.xml>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeRaidCfg --file
RAIDCfg.xml
```

In-band:

```
[SUM_HOME]# ./sum -c ChangeRaidCfg --file RAIDCfg.xml
```

5.8.5 Getting SATA HDD Information (OOB Only)

Use the command “GetSataInfo” to get the current SATA HDD information under on-board AHCI controller from the managed system.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c GetSataInfo
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSataInfo
```

The console output contains the following information.

```
SATA HDD Information
====================
    [HDD(0)]
            Controller Name: PCH SATA
            Configuration Type: AHCI
            Slot ID: 0
            Slot Populated: Yes
            Model Name: INTEL SSDSC2BB120G4
            Serial Number: PHWL542502J2120LGN
            HDD Firmware Version: D201037
            S.M.A.R.T. Supported: Yes
```

5.8.6 Getting NVMe Information

Use the command “GetNvmeInfo” to get the current NVMe information from the managed system.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c GetNvmeInfo [--dev_id
<device_id> ]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetNvmeInfo --dev_id
0
```

The console output contains the following information.

```
NVMe Device information
=======================
  [NVMe Controller(1)]
    [Group(1)]
      Group ID: 0
      [NVMe SSD(1)]
        Slot: 0
        Temperature: 37 degree C
        Device Class: Mass storage controller
        Device SubClass: Non-Volatile memory controller
        Device Program Interface: NVM express
        Vendor Name: Samsung Electronics Co., Ltd.
        Serial Number: S1NONYAF800079
        Model Number: MZWEI400HAGM-0003
        Port 0 Max Link Speed: 8 GT/s
        Port 0 Max Link Width: x4
        Port 1 Max Link Speed: N/A
        Port 1 Max Link Width: N/A
        Initial Power Requirement: 10 Watts
        Max Power Requirement: 25 Watts
        Located Status: Not Located
```

5.8.7 Secure Erasing Hard Disks

Use the command "SecureEraseDisk" to have SUM securely erase an HDD on the managed system. After a secure erase is complete, the HDD is formatted and its password is cleared. An HDD without a password installed can be securely erased directly without a password or PSID. It is recommended that an HDD password should be immediately installed after the HDD is securely erased. The "SecureEraseDisk" command can be used to install the HDD password if no passwords are installed on the HDD.

Currently, SUM supports the secure-erase feature in three security modes: TCG, SAT3 and Not TCG/SAT3 Supported. The supported actions of SecureEraseDisk command are shown in the following table.

Security Mode	Action	Description
TCG Supported	SetPassword	Sets an HDD password
	ChangePassword	Changes the HDD password
	ClearPassword	Clears the HDD password
	SecurityErase	Erases a device without an HDD password installed. If an HDD password is installed, the device cannot be erased.
	SecurityErasePWD	Erases a device with an HDD password.
	SecurityErasePSID	Erases a device with PSID.
SAT3 Supported	SetPassword	Sets up an HDD password.
	ChangePassword	Changes the HDD password
	ClearPassword	Clears the HDD password
	SecurityErase	Erases a device without an HDD password installed. If an HDD password is installed, a device cannot be erased.
	SecurityErasePWD	Erases a device with an HDD password. An HDD password must be installed before secure erase.
Not TCG/SAT3 Supported	SecurityErase	Erases a device without an HDD password installed. If an HDD password is installed, a device cannot be erased.

The SecureEraseDisk command needs two format types of input files for different types of secure erase:

- **PSID.txt**: serial number;PSID. Note that a PSID can be found on the sticker of a TCG device.
- **Password.txt**: serial number; password; new_password. Note that the "new_password" is required for the action ChangePassword. This field is optional for other actions.

SUM maps the PSID and password to the target HDD on the managed system automatically based on serial numbers. The following is an example of PSID.txt and Password.txt:

Assume there is a system installed with one SAT3 supported device and one TCG supported device:

Security Mode	Serial Number	PSID	Password	New Password
SAT3	9XF4AF7M	N/A	123456	111111
TCG	W472TJXH	HR1MJDCKLH4CD88ELEGDUE5J4UA3QGZZ	123456	111111

PSID.txt

```
W472TJXH;          HR1MJDCKLH4CD88ELEGDUE5J4UA3QGZZ
```

Password.txt

```
9XF4AF7M;          123456;    111111

W472TJXH;          123456;    111111
```

Execution Modes

5.8.7.1 The SecureEraseDisk command has two execution modes: Action Mode and Pre-check Mode

- **Action Mode:** Action mode supports the following actions, requiring the managed system to be reboot for changes to take effect.
  - **SetPassword:** Sets an HDD password.
  - **ChangePassword:** Changes the HDD password
  - **ClearPassword:** Clears the HDD password
  - **SecurityErase:** Securely erases the HDD with no password installed.
  - **SecurityErasePWD:** Securely erases the HDD with the installed HDD password.
  - **SecurityErasePSID:** Securely erases the HDD with a PSID.
- **Pre-check Mode** shows the information below.
  - **HDD Password Status:** Shows if a password is installed on the HDD.
  - **Security Mode:** Shows the security mode that HDD supports and indicates supported actions by the device.
  - **TCG Device Type**: Shows the device type for the TCG supported HDD.
  - **Applicable Actions:** Shows the actions which can be executed on the HDD.
  - **Estimated Execution Time for Secure Erase:** Shows the estimated execution time for securely erasing one or more HDDs on the managed system.
  - **No Matched HDDs:** This type of information is recorded in a text file named PreCheckFile. No matched HDDs could be a result of failed matches between HDDs in the serial number mapping file and the managed system.

It is recommended that the pre-check mode should be run before a secure erase. Note that some types of HDDs take a longer time to be securely erased, and an HDD can only be securely erased after another erase task is finished.

Securely Erasing an HDD

1. Run the command to check the HDD supported actions and get the erase time. The file “PreCheckfile” will be created, whichincludes all unmapped hard disks. Note that the PSID.txt is only supported by TGC devices.

5.8.7.2

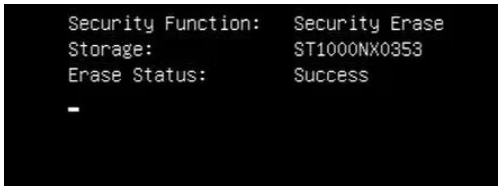
```
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file PSID.txt --
precheck
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file Password.txt --
precheck
Managed system.....192.168.34.56
[HDD]
    Serial Number ..................9XF4AF7M
    Password Status ................NOT INSTALLED
    Security Mode ..................SAT3 Supported
    Applicable Action..............SetPassword
                     ..............SecurityErase
[HDD]
    Serial Number..................W472TJXH
    Password Status................NOT INSTALLED
    Security Mode..................TCG Supported
    TCG Device Type................TCG-Enterprise
    Applicable Action..............SetPassword
                     ..............SecurityErase

Estimated security erase time......2 Minutes
Please check PreCheckFile for the mismatched HDDs.
```

2. Run the command based on the precheck result to securely erase an HDD. The action SecurityErase can accept both PSID.txt and Password.txt as an input file.

```
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file PSID.txt --action
SecurityErasePSID --reboot
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file Password.txt --
action SecurityErasePWD --reboot
```

3. The monitoring result of the managed system appears.



4. After the task is complete, use the command SUM GetCurrentBiosCfg to check the result through BIOS configurations. Find the status code by the following key word. For details on the command "GetCurrentBiosCfg", see *5.3.3 Receiving Current BIOS Settings*.

   Text = "Last Status Code". A status code of zero indicates the previous task was successful.

5.8.7.3 Setting a HDD Password

1. Run the command to check the HDD supported actions. Note that another password cannot be assigned to an HDD with a password already installed. The file "PreCheckfile" will be created, which includes all unmapped HDDs.

```
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file Password.txt --
precheck
Managed system.....192.168.34.56
[HDD]
    Serial Number ..................9XF4AF7M
    Password Status ................NOT INSTALLED
    Security Mode ..................SAT3 Supported
    Applicable Action..............SetPassword
                    ..............SecurityErase
[HDD]
    Serial Number..................W472TJXH
    Password Status................NOT INSTALLED
```

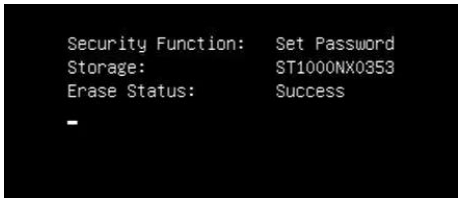
```
        Security Mode..................TCG Supported
        TCG Device Type................TCG-Enterprise
        Applicable Action..............SetPassword
                                       ..............SecurityErase

    Estimated security erase time......2 Minutes
    Please check the PreCheckFile for the mismatched HDDs.
```

2. Run the command to set an HDD password.

```
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file Password.txt --
action SetPassword --reboot
```

3. The monitoring result of the managed system appears.



4. After the task is complete, to check the execution result, run the command SUM GetCurrentBiosCfg (see *5.3.3 Receiving Current BIOS Settings*), and then type Text = “Last Status Code” to find the status code in the BIOS configurations.
   . A status code of zero indicates the previous task was successfull. For non-zero status codes, please refer to *Appendix D - Status Codes* in *UEFI Specification 2.8*.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SecureEraseDisk --file
<filename> [[--action <action> --reboot] | [--precheck]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureEraseDisk --
file Password.txt --precheck
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureEraseDisk --
file Password.txt --action SetPassword --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureEraseDisk --
file Password.txt --action SecurityErase --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c SecureEraseDisk --file PSID.txt --precheck

[SUM_HOME]# ./sum -c SecureEraseDisk --file Password.txt --action
SecurityErasePWD --reboot

[SUM_HOME]# ./sum -c SecureEraseDisk --file PSID.txt --action SecurityErasePSID
--reboot
```

The console output for --precheck option contains the following information.

```
Managed system.....192.168.34.56
[HDD]
    Serial Number ..................S45RNE0M600194
    Password Status ................NOT INSTALLED
    Security Mode ..................SAT3 Supported
    Applicable Action..............SetPassword
                     ..............SecurityErase
[HDD]
    Serial Number..................W472TJXH
    Password Status................INSTALLED
    Security Mode..................TCG Supported
    TCG Device Type................TCG-Enterprise
    Applicable Action..............SecurityErasePWD
                     ..............SecurityErasePSID
                     ..............ChangePassword
                     ..............ClearPassword
```

```
Estimated security erase time......33 Minutes

Please check PreCheckFile for the mismatched HDDs.
```

Notes:

- A Password/PSID file follows the CSV format with ; (a semicolon).
- The SecureEraseDisk command requires either of the options --action or --precheck.
- By default, the NVMe vendor's driver will be loaded by BIOS to provide more information, but when loaded, the storage cannot be securely erased by BIOS. The user needs to switch to the native AMI driver manually by changing the BIOS setting "NVMe Firmware Source" to "AMI Native Support". If there is no "NVMe Firmware Source" setting under BIOS configuration, please try to change the BIOS setting "Onboard NVMe Option ROM" to "Disabled".
- An HDD without a password installed can be securely erased without a password or a PSID, so it is recommended that a password be assigned to the hard disk.
- Another password cannot be assigned to the HDD with a password installed by SetPassword action.
- Some BIOS may be in the Security Mode: "NONE". This is the same as "Not TCG/SAT3 Supported".
- There are limitations for some BIOS:
  - TCG supported devices can only be securely erased by the command "SecurityErasePSID".
  - SAT3 supported devices can only be securely erased by the command "SecurityErasePWD," and the HDD password has to be installed before the HDD is erased.
  - Some BIOS might not support security features for "Not TCG/SAT3 Supported" device.
- The estimated time length for securely erasing an HDD:
  - 500GB SATA HDD: 98 minutes
  - 128GB SSD: 2 minutes
  - 512GB NVMe: a few seconds
- The SecureEraseDisk command is supported by the following platforms:
  - X11 2nd Generation Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets
  - X11 8th/9th Generation Intel® CoreTMi3/Pentium®/Celeron® Processor, X11 Intel® Xeon® E-2100 Processor and X11 Intel® Xeon® E-2200 Processor with Intel® C246/C242 chipset
  - H11 AMD EPYC
  - X12/H12 and later platforms

5.8.8 Securely Erasing Hard Disks in LSI MegaRaid SAS 3108 RAID Controller

Use the command “SecureEraseRaidHdd” to execute SUM to securely erase hard disks (HDD or SSD) in the target LSI MegaRaid SAS 3108 RAID controller system and poll the erasing status asynchronously or synchronously.

Syntax:

```
1. sum -i <IP or host name> -u <username> -p <password> -c SecureEraseRaidHdd

--dev_id <device_id> --enc_id <enclosure id> --dsk_id <disk id> [--sync]

2. sum -i <IP or host name> -u <username> -p <password> -c SecureEraseRaidHdd

--tsk_id <task id> [--sync]
```

To securely erase HDDs in the LSI MegaRaid SAS 3108 RAID controller system, follow these steps .

1. Execute the command “GetRaidCfg” to confirm the JBOD mode of the LSI MegaRaid SAS 3108 RAID controller system is in “Disabled” state, and the disks to be erased in the LSI MegaRaid SAS 3108 RAID controller system are in “Unconfigured good drive” state. After checking, you can decide your target physical disk ID(s) based on the configuration in the LSI MegaRaid SAS 3108 RAID controller system.
2. Follow the rule below to erase your target physical disk(s) listed in the LSI MegaRaid SAS 3108 RAID controller system.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c SecureEraseRaidHdd

--dev_id <device_id> --enc_id <enclosure id> --dsk_id <disk id> [--sync]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureEraseRaidHdd

--dev_id 0 --enc_id 0,1 --dsk_id 0,1,2,3
```

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.6.0 (2021/04/29) (x86_64)

Copyright(C) 2013-2021 Super Micro Computer, Inc. All rights reserved.

Warning: Please make sure the F/W State of each disk is in "Unconfigured good
drive" state.

Otherwise, please

(1) Delete your virtual disk(VD) if any.

    Or

(2) Disable JBOD mode if set before.

Checking FW state of each disk...

The F/W STATE of EACH DISK :

[--dev_id:--enc_id:--dsk_id] : F/W State

[ 0: 0: 0] : Unconfigured good drive

[ 0: 0: 1] : Unconfigured good drive

[ 0: 0: 2] : Configured-drive is online

[ 0: 0: 3] : Configured-drive is online

[ 0: 1: 0] : Unconfigured good drive

[ 0: 1: 1] : Unconfigured good drive

*********************************<<<<<ERROR>>>>>**********************************

      ExitCode               = 153
      Description            = IPMI execution on non-supported device
      Program Error Code     = 440.21
```

```
Error message:
        The F/W state:
        Enclosure ID: 0 Disk ID: 2
        Enclosure ID: 0 Disk ID: 3
        are not allowed to be securely erased.
Instruction:
        Please check the F/W state of unallowed disks and try again.

*********************************************************************************
```

SUM will check the firmware state of each target disk first. If the status is not "Unconfigured good drive", the execution will stop. After double-checking the target disks' firmware state and running the same command again, the output will list results of all target disks with their task IDs and messages. There are three types of result messages for different HW/SW situations. The result levels are from good to bad and marked in blue, orange, and red colors.

Result Messages of Secure Erase	Situation				Target Disk Firmware State
	Secure Erase Already Started	LSI MegaRaid SAS 3108 RAID Controller JBOD Mode	Configured as VD	BMC Error Response	
"Start polling progress."	NO	Disabled	NO	NO	Unconfigured good drive
"Already started polling progress."	YES	Disabled	NO	NO	Unconfigured good drive
"Action not allowed. Please check the controller or disk status."	NO	Disabled	NO	YES	Unconfigured good drive
	NO	Enabled	NO	NO	Drive is exposed and controlled by a host.
	NO	Disabled	YES	NO	The configured drive is online.

If the target disk is accepted for secure erase or it is being securely erased, there will be a task ID. If the target disk is not allowed for secure erase, there is no task ID. Please remember the task ID(s) for futher polling status purpose.

You can also poll the erasing status right after issuing the command by appending --sync option after the command “SecureEraseRaidHdd”.

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureEraseRaidHdd

--dev_id 0 --enc_id ALL --dsk_id 0,1,2,3 --sync
```

- **Note:** For Windows, the argument value can be put into either double quotation marks or not. Example: `--enc_id “ALL”` or `--enc_id ALL`.

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.6.0 (2021/04/29) (x86_64)

Copyright(C) 2013-2021 Super Micro Computer, Inc. All rights reserved.

Warning: Please make sure the F/W State of each disk is in "Unconfigured good
drive".

Otherwise, please

(1) Delete your virtual disk(VD) if any.

    Or

(2) Disable JBOD mode if set before.

Checking FW state of each disk...

The F/W STATE of EACH DISK :
```

```
[--dev_id:--enc_id:--dsk_id] : F/W State

[ 0: 0: 0] : Unconfigured good drive

[ 0: 0: 1] : Unconfigured good drive

[ 0: 0: 2] : Unconfigured good drive

[ 0: 0: 3] : Unconfigured good drive

[ 0: 1: 0] : Unconfigured good drive

[ 0: 1: 1] : Unconfigured good drive

..............................

SECURE ERASE RESPONSE :

[--dev_id:--enc_id:--dsk_id:--tsk_id] : MESSAGE

[ 0: 0: 0:  1] : Already started polling progress.

[ 0: 0: 1:  2] : Already started polling progress.

[ 0: 0: 2:  3] : Start polling progress.

[ 0: 0: 3:  4] : Start polling progress.

[ 0: 1: 0:  5] : Start polling progress.

[ 0: 1: 1:  6] : Start polling progress.

Secure-Erase progress is starting...

-------------------------RAID Controller Task Service-------------------------

 Tsk | Raid | Enc | Dsk | Progress |     State | Start Time |  Elapsed |

   1 |    0 |   0 |   0 |      72% |   Running |

   2 |    0 |   0 |   1 |      73% |   Running |
```

```
   3 |    0 |   0 |   2 |       4% |   Running |

   4 |    0 |   0 |   3 |       4% |   Running |

   5 |    0 |   1 |   0 |       4% |   Running |

   6 |    0 |   1 |   1 |       4% |   Running |

Polling progress...
```

3. Excute the command “SecureEraseRaidHdd” with the --tsk_id option below to check the erasing status of target disk(s) in the LSI MegaRaid SAS 3108 RAID system.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c SecureEraseRaidHdd

--tsk_id <task id> [--sync]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureEraseRaidHdd

--tsk_id 1,2,3,4,5,6 --sync
```

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.6.0 (2021/04/29) (x86_64)

Copyright(C) 2013-2021 Super Micro Computer, Inc. All rights reserved.

-------------------------RAID Controller Task Service-------------------------

 Tsk | Raid | Enc | Dsk | Progress |     State | Start Time |  Elapsed |

   1 |    0 |   0 |   0 |      74% |   Running |

   2 |    0 |   0 |   1 |      75% |   Running |

   3 |    0 |   0 |   2 |       8% |   Running |
```

```
   4 |    0 |   0 |   3 |       8% |   Running |

   5 |    0 |   1 |   0 |       7% |   Running |

   6 |    0 |   1 |   1 |       7% |   Running |

Polling progress...
```

If the task status becomes “Completed”, the start and elapsed time of task will appear on the console output.

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureEraseRaidHdd

--tsk_id 1,2,3,4,5,6 --sync
```

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.6.0 (2021/04/29) (x86_64)

Copyright(C) 2013-2021 Super Micro Computer, Inc. All rights reserved.


------------------------RAID Controller Task Service-------------------------

 Tsk | Raid | Enc | Dsk | Progress |     State | Start Time |  Elapsed |

   1 |    0 |   0 |   0 |     100% | Completed |   12:53:43 | 02:44:13 |

   2 |    0 |   0 |   1 |     100% | Completed |   12:54:17 | 02:44:13 |

   3 |    0 |   0 |   2 |     100% | Completed |   14:32:47 | 02:45:13 |

   4 |    0 |   0 |   3 |     100% | Completed |   14:32:55 | 02:45:13 |

   5 |    0 |   1 |   0 |     100% | Completed |   14:33:17 | 02:46:13 |

   6 |    0 |   1 |   1 |     100% | Completed |   14:33:25 | 02:46:13 |
```

```
Secure-Erase progress Done.
```

- **Note:** The SecureEraseRaidHdd command is supported on X12/H12 and later platforms .

5.8.9 Getting PMem Firmware Image Information

Use the command “GetPMemInfo” to receive the PMem firmware image information from the managed system as well as the local PMem firmware image (with the option --file).

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
GetPMemInfo [--file <filename> [--file_only]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetPMemInfo
```

The console output contains the following information.

```
Managed system.................192.168.34.56
    PMem version..............2.2.0.1464
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetPMemInfo --file
PMem.bin
```

The console output contains the following information.

```
Managed system.................169.254.3.254
    PMem version..............2.2.0.1464
Local PMem image file.........PMem.bin
    PMem version..............2.2.0.1469
```

```
[SUM_HOME]# ./sum -c GetPMemInfo --file PMem.bin --file_only
```

The console output contains the following information.

```
Local PMem image file..........PMem.bin
    PMem version..............2.2.0.1469
```

Notes:

- This command is available on X12 3rd Gen Intel® Xeon® Scalable processors with Intel® C621A Series Chipsets and later platforms.
- The PMem firmware version retrieved from the “GetPMemInfo” command is the running PMem firmware version.
- For more detailed usages of PMem, please contact Supermicro technical support.

5.8.10 Updating the PMem Firmware Image

Use the command “UpdatePMem” with the PMem firmware image PMem.bin to run SUM to update the PMem of managed system.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
UpdatePMem [[--file <filename>] | [--restore_default_fw]] [--reboot]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdatePMem --file
PMem.bin --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdatePMem --file
PMem.bin --reboot

[SUM_HOME]# ./sum -c UpdatePMem --restore_default_fw -reboot
```

Notes:

- This command is available on the X12 3rd Gen Intel® Xeon® Scalable processors with Intel® C621A Series Chipsets and later platforms.
- For more detailed usages of PMem, please contact the technical support of Supermicro.

5.9 PSU Management for a Single System

5.9.1 Getting PSU Information

Use the command “GetPsuInfo” to get the current PSU information from the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetPsuInfo
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetPsuInfo
```

In-Band:

```
[SUM_HOME]# ./sum -c GetPsuInfo
```

The console output contains the following information.

```
[Module 1](SlaveAddress = 0x78)
    PWS Module Number: PWS-605P-1H
    PWS Serial Number: P605A0E39B07611
    PWS Revision: REV1.1
    PMBus Revision: 0x8B22
    Status: [STATUS OK](00h)
    AC Input Voltage: 122.00 V
    AC Input Current: 0.46 A
    DC 12V Output Voltage: 12.38 V
    DC 12V Output Current: 4.50 A
    Temperature 1: 25 C
    Temperature 2: 53 C
    Fan 1: 2688 RPM
    Fan 2: N/A
    DC 12V Output Power: 55 W
    AC Input Power: 55 W
```

5.9.2 Updating the Signed PSU Firmware Image Requested by OEM

Use the command “UpdatePsu” with a signed PSU firmware image requested by OEM and the PSU slave address to run SUM to update the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c UpdatePsu --file
<filename> --address <PSU slave address>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdatePsu --file
SMCI_PSU.x0 --address 0x80
```

In-Band:

```
[SUM_HOME]# ./sum -c UpdatePsu --file SMCI_PSU.x0 --address 0x80
```

Notes:

- During PSU firmware updating process, the updated PSU will be powered off. Therefore, system needs to connect to at least two PSUs to support this command.
- Slave address of the PSU that needs to be updated can be found by executing “GetPsuInfo” command.
- The updated PSU will be rebooted automatically when firmware update completes.
- PSU updated on the system with LCMC is only supported on X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms.

5.9.3 Getting Current Power Status of Managed System

Use the command “GetPowerStatus” to get the current power status of the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetPowerStatus
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetPowerStatus
```

The console output contains the following information.

```
Managed system.................192.168.34.56

    Power status..............On
```

In-Band:

```
[SUM_HOME]# ./sum -c GetPowerStatus
```

The console output contains the following information.

```
Managed system.................localhost

    Power status..............On
```

5.9.4 Setting Power Action of Managed System

Use the command “SetPowerAction” to set the type of power action of the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetPowerAction --
action <action> --blade [<Blade_Index> | ALL] [--node <Node Index>]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetPowerAction --
action up
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetPowerAction --
action 0
```

In-Band:

```
[SUM_HOME]# ./sum -c SetPowerAction --action up

[SUM_HOME]# ./sum -c SetPowerAction --action 0
```

The console output contains the following information.

```
Going to power up the managed system.
```

5.10 TPM Management for a Single System

Before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, the command "TpmProvision" can be executed to enable TPM module capabilities and clear TPM module capabilities for the managed system.

For X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, through OTA TPM technologies, the commands "GetTpmInfo" and "TpmManage" can be executed to receive TPM information and manage TPM, respectively. Since SUM 2.2.0, SUM has two implementations for OTA TPM management: Intel OTA and SMCI OTA. Depending on product design, either solution is implemented for the managed system. Supported OTA solution can be obtained on the output of the command "GetTpmInfo". For more detailed information, please contact technical support.

The detailed information of TPM features are listed in the tables below.

Command	Management Interface Supported		Node Product Key Required on the Managed System (SFT-OOB-LIC, or SFT-DCMS-SINGLE)
	Out-Of-Band (Remote)	In-Band (Local)	
TpmProvision	**Yes**	No	Required
GetTpmInfo (SMCI OTA)	**Yes**	**Yes**	Required
GetTpmInfo (Intel OTA)	**Yes**	**Yes**	Required
TpmManage (SMCI OTA)	**Yes**	**Yes**	Required
TpmManage (Intel OTA)	**Yes**	**Yes**	Required

SUM (OOB & In-Band) Solution Feature	HW & FW Compatibility		
	Without BMC	With BMC	
	Platform supported listed in the "With BMC columns"	Before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets platforms	X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms
TpmProvision	No	**Yes**	No
GetTpmInfo (SMCI OTA)	No	No	**Yes**
GetTpmInfo (Intel OTA)	No	No	**Yes**
TpmManage (SMCI OTA)	No	No	**Yes**
TpmManage (Intel OTA)	No	No	**Yes**

5.10.1 Getting TPM Information

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the command "GetTpmInfo" to receive the TPM module information from the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetTpmInfo [--showall]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetTpmInfo --showall
```

In-Band:

```
[SUM_HOME]# ./sum -c GetTpmInfo --showall
```

The console output contains the following information when installing the TPM 1.2 module.

```
Supermicro Update Manager (for UEFI BIOS) 2.1.0 (2018/02/09) (x86_64)
Copyright(C)2018 Super Micro Computer, Inc. All rights reserved.
Query through SMCI OTA


TPM Information
================
    TXT Support: Yes
    TPM Support: dTPM supported
    TXT Status: Disabled
    dTPM Status: Enabled
    fTPM Status: Disabled
    TPM Version: TPM 1.2
    TPM Provisioned: Yes
    TPM Ownership: No
    TPM PS NV Index write-protected: No
```

```
    TPM AUX NV Index write-protected: No
    TPM PO NV Index write-protected: No
    TPM Locked: Yes
```

The following information is displayed only when the command "GetTpmInfo" is executed with the option "--showall". Only the SMCI OTA solution supports the option "--showall".

```
TPM 1.2 PS NV index LCP Definition
==================================
    [NV Public Data]
        Tag: 0x0018
        NV index: 0x50000001
        ReadSizeOfSelect: 0x0003
        ReadPCRSelect[0]: 0x00
        ReadPCRSelect[1]: 0x00
        ReadPCRSelect[2]: 0x00
        ReadLocalityAtRelease: 0x1F

        ReadDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00

        WriteSizeOfSelect: 0x0003
        WritePCRSelect[0]: 0x00
        WritePCRSelect[1]: 0x00
        WritePCRSelect[2]: 0x00
        WriteLocalityAtRelease: 0x1F

        WriteDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
```

```
        Tag1: 0x0017
        Attributes: 0x00002000
        bReadSTClear: 0x00
        bWriteSTClear: 0x00
        bWriteSDefine: 0x01

        LCP Policy:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 20 32 63
        66 33 65 39 E1 00 00 00 00 00 00 00 10 0E 39 02
        00 00 00 00 88 78

TPM 1.2 AUX NV index LCP Definition
==================================
    [NV Public Data]
        Tag: 0x0018
        NV index: 0x50000003
        ReadSizeOfSelect: 0x0003
        ReadPCRSelect[0]: 0x00
        ReadPCRSelect[1]: 0x00
        ReadPCRSelect[2]: 0x00
        ReadLocalityAtRelease: 0x1F

        ReadDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00

        WriteSizeOfSelect: 0x0003
        WritePCRSelect[0]: 0x00
        WritePCRSelect[1]: 0x00
        WritePCRSelect[2]: 0x00
        WriteLocalityAtRelease: 0x18
```

```
        WriteDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00

        Tag1: 0x0017
        Attributes: 0x00000000
        bReadSTClear: 0x00
        bWriteSTClear: 0x00
        bWriteSDefine: 0x00

        LCP Policy:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

TPM 1.2 PPI NV index LCP Definition
===================================
    [NV Public Data]
        Tag: 0x0018
        NV index: 0x50010000
        ReadSizeOfSelect: 0x0003
        ReadPCRSelect[0]: 0x00
        ReadPCRSelect[1]: 0x00
        ReadPCRSelect[2]: 0x00
        ReadLocalityAtRelease: 0x1F

        ReadDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
```

```
        WriteSizeOfSelect: 0x0003
        WritePCRSelect[0]: 0x00
        WritePCRSelect[1]: 0x00
        WritePCRSelect[2]: 0x00
        WriteLocalityAtRelease: 0x1F

        WriteDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00

        Tag1: 0x0017
        Attributes: 0x00000001
        bReadSTClear: 0x00
        bWriteSTClear: 0x00
        bWriteSDefine: 0x00

        LCP Policy:
        00 00 00 00 00 00 00 00 00 00

TPM 1.2 Capability Flags
========================
    [Volatile Flags]
        deactivated: 0
        disableForceClear: 0
        physicalPresence: 0
        physicalPresenceLock: 1
        bGlobalLock: 0

    [Permanent Flags]
        disable: 0
        ownership: 1
        deactivated: 0
        readPubEK: 1
```

```
        disableOwnerClear: 0
        allowMaintenance: 0
        physicalPresenceLifetimeLock: 0
        physicalPresenceHWEnable: 0
        physicalPresenceCMDEnable: 1
        FIPS: 0
        enableRevokeEK: 0
        nvLocked: 1
        tpmEstablished: 0
```

The console output contains the following information when installing the TPM 2.0 module.

```
Supermicro Update Manager (for UEFI BIOS) 2.1.0 (2018/02/09) (x86_64)
Copyright(C)2018 Super Micro Computer, Inc. All rights reserved.
Query through SMCI OTA


TPM Information
================
    TXT Support: Yes
    TPM Support: dTPM supported
    TXT Status: Enabled
    dTPM Status: Enabled
    fTPM Status: Disabled
    TPM Version: TPM 2.0
    TPM Provisioned: Yes
    TPM Ownership: No
    TPM PS NV Index write-protected: No
    TPM AUX NV Index write-protected: No
    TPM PO NV Index write-protected: No
```

The following information is displayed only when the GetTpmInfo is executed with option "--showall". Only SMCI OTA solution supports option "--showall".

```
TPM 2.0 PS NV index LCP Definition
==========================
    [NV Public Data]
        NvIndex: 0x01C10103
        NameAlg: SHA256
        Attributes: 0x62040408
        PPWrite: 0
        OWNERWrite: 0
        AuthWrite: 0
        PolicyWrite: 1

        Counter: 0
        Bits: 0
        Extend: 0
        PolicyDelete: 1
        WriteLocked: 0
        WriteAll: 0
        WriteDefine: 0
        WriteStClear: 0
        GlobalLock: 0
        PPRead: 0
        OwnerRead: 0
        AuthRead: 1
        PolicyRead: 0
        NoDA: 1
        Orderly: 0
        ClearStClear: 0
        ReadLocked: 0
        Written: 1
```

```
        PolicyRead: 0
        PlatformCreate: 1
        ReadStClear: 0

        AuthPolicy Digest:
        C0 01 C8 00 02 10 D0 FA A4 F4 F4 F8 A7 8E F4 F8
        26 4E 6F 85 55 34 0D 2F 04 18 0F 8C F1 10 FF DD

        Name:
        00 0B 40 7B A7 8D 90 B7 CF 3A A5 3C 0B 83 6D AE
        A7 2A E6 B5 67 15 32 BD 4E EF E4 04 E3 7E A4 EB
        B0 19

        LCP Policy:
        00 03 0B 00 01 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 02 00 00 00 00 00 C8 00 08 30
        00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00

TPM 2.0 AUX NV index LCP Definition
============================
    [NV Public Data]
        NvIndex: 0x01C10102
        NameAlg: SHA256
        Attributes: 0x62044408
        PPWrite: 0
        OWNERWrite: 0
        AuthWrite: 0
        PolicyWrite: 1
        Counter: 0
        Bits: 0
        Extend: 0
```

```
PolicyDelete: 1
WriteLocked: 0
WriteAll: 0
WriteDefine: 0
WriteStClear: 1
GlobalLock: 0
PPRead: 0
OwnerRead: 0
AuthRead: 1
PolicyRead: 0
NoDA: 1
Orderly: 0
ClearStClear: 0
ReadLocked: 0
Written: 1
PolicyRead: 0
PlatformCreate: 1
ReadStClear: 0

AuthPolicy Digest:
EF 9A 26 FC 22 D1 AE 8C EC FF 59 E9 48 1A C1 EC
53 3D BE 22 8B EC 6D 17 93 0F 4C B2 CC 5B 97 24

Name:
00 0B 87 7A 0A B0 02 23 4B C3 A3 61 5C 81 9A BF
20 C3 0A 5F 2A F9 3F B6 DC 13 F3 B9 B0 59 90 F4
5A FB

LCP Policy:
00 00 00 00 11 09 17 20 07 B0 00 00 00 02 00 00
00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00
CA D5 6B 67 FD 9A 84 36 B6 69 0B 50 8F 34 95 94
```

```
        95 AD 11 69 8A 2D 9A DE 0F 3D F5 DF A3 6A 0A 5C
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00

TPM 2.0 SGX NV index LCP Definition
===========================
    [NV Public Data]
        NvIndex: 0x01C10104
        NameAlg: SHA256
        Attributes: 0x62040404
        PPWrite: 0
        OWNERWrite: 0
        AuthWrite: 1
        PolicyWrite: 0
        Counter: 0
        Bits: 0
        Extend: 0
        PolicyDelete: 1
        WriteLocked: 0
        WriteAll: 0
        WriteDefine: 0
        WriteStClear: 0
        GlobalLock: 0
        PPRead: 0
        OwnerRead: 0
        AuthRead: 1
        PolicyRead: 0
        NoDA: 1
        Orderly: 0
        ClearStClear: 0
```

```
        ReadLocked: 0
        Written: 1
        PolicyRead: 0
        PlatformCreate: 1
        ReadStClear: 0

        AuthPolicy Digest:
        B7 5C E1 94 6F 78 DF 8B AA 42 69 18 DB 09 31 80
        17 E6 B3 8D 04 8C 95 4E 05 C2 C4 F3 4B D4 40 60

        Name:
        00 0B 3E CE D2 44 B7 B3 E8 33 3D A2 A8 C5 5E 9A
        40 22 02 E1 C4 45 E8 D3 5D EE 0F C5 EE 17 8A 05
        54 53

        LCP Policy:
        01 00 00 00 00 00 00 00

TPM 2.0 PPI NV index LCP Definition
============================
    [NV Public Data]
        NvIndex: 0x01C10105
        NameAlg: SHA256
        Attributes: 0x42040409
        PPWrite: 1
        OWNERWrite: 0
        AuthWrite: 0
        PolicyWrite: 1
        Counter: 0
        Bits: 0
        Extend: 0
        PolicyDelete: 1
        WriteLocked: 0
```

```
        WriteAll: 0
        WriteDefine: 0
        WriteStClear: 0
        GlobalLock: 0
        PPRead: 0
        OwnerRead: 0
        AuthRead: 1
        PolicyRead: 0
        NoDA: 1
        Orderly: 0
        ClearStClear: 0
        ReadLocked: 0
        Written: 0
        PolicyRead: 0
        PlatformCreate: 1
        ReadStClear: 0

        AuthPolicy Digest:
        B7 5C E1 94 6F 78 DF 8B AA 42 69 18 DB 09 31 80
        17 E6 B3 8D 04 8C 95 4E 05 C2 C4 F3 4B D4 40 60

        Name:
        00 0B 5B 53 B9 80 E7 36 D4 C3 3B 85 A6 A2 BB 7A
        A5 F6 D3 10 1C EB D3 17 7D 69 8E D1 84 51 02 E2
        D0 1B

TPM 2.0 PO NV index LCP Definition
==========================
    [NV Public Data]
        NvIndex: 0x01C10106
        NameAlg: SHA256
        Attributes: 0x2204000A
```

```
PPWrite: 0
OWNERWrite: 1
AuthWrite: 0
PolicyWrite: 1
Counter: 0
Bits: 0
Extend: 0
PolicyDelete: 0
WriteLocked: 0
WriteAll: 0
WriteDefine: 0
WriteStClear: 0
GlobalLock: 0
PPRead: 0
OwnerRead: 0
AuthRead: 1
PolicyRead: 0
NoDA: 1
Orderly: 0
ClearStClear: 0
ReadLocked: 0
Written: 1
PolicyRead: 0
PlatformCreate: 0
ReadStClear: 0

AuthPolicy Digest:
22 03 0B 7E 0B B1 F9 D5 06 57 57 1E E2 F7 FC E1
EB 91 99 0C 8B 8A E9 77 FC B3 F1 58 B0 3E BA 96

Name:
00 0B 8D D1 B6 DE A2 9D 5B 82 D7 1B 04 84 83 D6
```

```
A9 BF DE B1 A9 34 46 AA 96 09 FF D6 AF BE BC 95
7C 19

LCP Policy:
00 03 0B 00 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 02 00 00 00 00 00 C8 00 08 30
00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00
```

Notes:

- This command is supported on X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets or later platforms.
- The field “TPM Locked” in “TPM Information” section is only for TPM 1.2.
- The section “Capability Flags” is only for TPM 1.2.
- The option --showall is optional for the GetTpmInfo command.
- The sections “PS NV INDEX LCP Definition”, “AUX NV INDEX LCP Definition”, “PPI NV INDEX LCP Definition” and “Capability Flags” will be displayed when the option --showall is assigned.
- This command will query TPM module information through Intel OTA or SMCI OTA.

5.10.2 Provisioning TPM Module

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the command "TpmManage" to execute SUM to enable TPM module capabilities for the managed system. Before executing the command, the TPM module should be installed on the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c TpmManage --provision
[options…]
```

Option Commands	Descriptions
--reboot	Forces the managed system to reboot or power up after operation.
--provision	Launches the trusted platform module provision procedure.
--table_default	Uses the default TPM provision table.
--table <file name>	Uses the customized TPM provision table.

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --provision
--table_default --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --provision
--table Tpm12Prov.bin --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c TpmManage --provision --table_default --reboot

[SUM_HOME]# ./sum -c TpmManage --provision --table Tpm12Prov.bin --reboot
```

Notes:

- This command is supported on X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets or later platforms.
- The system may be rebooted several times during provisioning.

- Please execute GetTpmInfo command to obtain OTA supported type before doing TPM provision.
- The TPM module will have been locked when the provisioning procedure is completed.
- Executing the TpmManage command with option --table_default will execute TPM provisioning with default TPM provision table created by BIOS.
- Executing TpmManage command with option --table will execute TPM provisioning with customized TPM provision table created by user.
- The --reboot option is required by the TPM provision procedure for OOB Intel OTA solutions.
- For TPM provision use with in-band Intel OTA, please follow these steps to complete TPM provision.
  a. Execute the command "TpmManage" with the option "--clear_and_enable_dtpm" and "--reboot" to enable TPM.
  b. Execute the command "TpmManage" with the option "--provision" to do TPM provision and then reboot the managed system manually.
  c. Execute the command "TpmManage" with the options "--enable_txt_and_dtpm" and "--reboot" to enable TPM and TXT.

On platforms before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, use the command "TpmProvision" to execute SUM to enable TPM module capabilities for the managed system. Before executing the command, the TPM module should be installed on the managed system.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c TpmProvision --image_url
<URL>  --reboot --lock <yes> [[--id <id for URL> --pw <password for URL>] | [--
id <id for URL> --pw_file <password file path>]]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmProvision --
image_url 'smb://192.168.35.1/MySharedPoint/MyFolder' --id smbid --pw smbpasswd
--reboot --lock yes

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmProvision --
image_url 'http://192.168.35.1/MySharedPoint/MyFolder' --id smbid --pw smbpasswd
--reboot --lock yes
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmProvision --
image_url '\\192.168.35.1\MySharedPoint\MyFolder\' --id smbid --pw_file
smbpasswd.txt --reboot --lock yes

smbpasswd.txt:
smbpasswd
```

Notes:

- The TpmProvision command is supported from the X10 Intel® Xeon® Processor E5 v3/v4 Product Family to the X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets platforms.
- The TPM ISO images are not included in the SUM package. This ISO image can be acquired from Supermicro. Each SUM release could require different ISO images as noted in SUM release notes. Please acquire correct TPM_version_YYYYMMDD.zip, unzip the zip file and get TPM ISO images for usage.
- With TPM ISO images, TPM capabilities can be enabled or cleared.
- The BIOS will be rebooted several times during provisioning.
- To clear TPM capability, see *5.10.3 Enabling and Clearing TPM Module Capabilities.*
- Space is prohibited for a SAMBA password. SUM will check the TPM module status on the managed system. If it is not installed or it has malfunctioned, the exit code 36/37 will be returned respectively. If the TPM is locked, the exit code 37 will be returned.
- The --cleartpm option clears the ownership of the TPM module.
- The --lock yes option locks the TPM module.
- SUM will stop TPM provision procedures if the CPU or platform does not support Intel Trusted Execution Technology (Intel TXT).

5.10.3 Enabling and Clearing TPM Module Capabilities

On platforms after X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, use the command "TpmManage" with the options in the following table to provide TPM module capabilities from the managed system.

Option Commands	Descriptions
--reboot (optional)	Forces the managed system to reboot.
--clear_and_enable_dtpm_txt	Clears dTPM ownership and activates dTPM/TXT.
--clear_dtpm	Clears dTPM ownership and disables dTPM for TPM 1.2. Clears dTPM ownership for TPM 2.0.
--enable_txt_and_dtpm	Enables TXT and dTPM.
--clear_and_enable_dtpm	Clears dTPM ownership, disables dTPM (for TPM 1.2 only) and activates dTPM.
--disable_dtpm	Disables dTPM.
--disable_txt	Disables TXT.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c TpmManage [options…]
[--reboot]
```

Example:

OOB :

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage
--clear_and_enable_dtpm_txt --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage
--clear_dtpm --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage
--enable_txt_and_dtpm --reboot
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage
--clear_and_enable_dtpm --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage
--disable_dtpm --reboot

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage
--disable_txt --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -c TpmManage --clear_and_enable_dtpm_txt --reboot

[SUM_HOME]# ./sum -c TpmManage --clear_dtpm --reboot

[SUM_HOME]# ./sum -c TpmManage --enable_txt_and_dtpm --reboot

[SUM_HOME]# ./sum -c TpmManage --clear_and_enable_dtpm --reboot

[SUM_HOME]# ./sum -c TpmManage --disable_dtpm --reboot

[SUM_HOME]# ./sum -c TpmManage --disable_txt --reboot
```

Notes:

- The options “--clear_and_enable_dtpm_txt” and “--enable_txt_and_dtpm” cannot be used when TPM is not provisioned.
- The option “--disable_dtpm” cannot be used when TXT is enabled.
- Please execute the “GetTpmInfo” command to obtain OTA supported type before doing TPM use cases.
- The “--reboot” option is optional for in-band usage. If executing a command without this option, the managed system will not reboot. Then SUM will remind the user to reboot manually.
- The options of each use are mutually exclusive.

On platforms before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, use the command “TpmProvision” with the options “--cleartpm” and “--reboot” to clear TPM module capabilities from the managed system. For usage of the “--image_url” option, refer to the notes in *5.10.2 Provisioning TPM Module.*

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c TpmProvision --image_url
<URL> [--id <id for URL> --pw <password for URL>] --cleartpm  --reboot
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmProvision --
image_url 'smb://192.168.35.1/MySharedPoint/MyFolder' --id smbid --pw smbpasswd
--cleartpm --reboot
```

Note: The TpmProvision command is supported from the X10 Intel® Xeon® Processor E5 v3/v4 Product Family to the X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets platform.

5.11 GPU Management

5.11.1 Getting GPU Information

Use the command “GetGpuInfo” to get the current NVIDIA GPU information from the managed system.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetGpuInfo
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetGpuInfo
```

In-Band:

```
[SUM_HOME]# ./sum -c GetGpuInfo
```

The console output contains the following information of the managed system with GPU installed.

NVIDIA GPU driver is loaded on the managed system…..

GPU information

==========

[GPU(1)]

Location: SXB3 (Riser)

Slot: 00

Board part number: 900-22080-0000-000

Serial number: 0324914053200

Marketing name: Tesla K80

Part number: 102D-885-A1

Memory vendor: Hynix

Memory part number: 161-0164-100

Build date: 20141203

Firmware version: 80.21.1B.00.01

GPU GUID: GPU-9d317734-507a-54e8-ebe4f73dc043

InfoROM version: 2080.0200.00.04

Primary temperature: 40 C

Power consumption: 26 W

The console output contains the following information for HGX2 system.

GPU information

==========

[HGX2 Baseboard(1)]

FPGA Image Version: 3.1

FPGA Loaded Image Index: 2

PEX8725 EEPROM Version: 1.6

Baseboard Revision: A02

Baseboard ID: 00

PCIe Retimer EEPROM Versions

PCIe Retimer #1 EEPROM Version: 2.0

PCIe Retimer #2 EEPROM Version: 2.0

PCIe Retimer #3 EEPROM Version: 2.0

PCIe Retimer #4 EEPROM Version: 2.0

PCIe Retimer #5 EEPROM Version: 2.0

PCIe Retimer #6 EEPROM Version: 2.0

PCIe Retimer #7 EEPROM Version: 2.0

PCIe Retimer #8 EEPROM Version: 2.0

PCIe Retimer #9 EEPROM Version: 2.1

PCIe Retimer VendorIDs

PCIe Retimer #1 VendorID: 111D

PCIe Retimer #2 VendorID: 111D

PCIe Retimer #3 VendorID: 111D

PCIe Retimer #4 VendorID: 111D

PCIe Retimer #5 VendorID: 111D

PCIe Retimer #6 VendorID: 111D

PCIe Retimer #7 VendorID: 111D

PCIe Retimer #8 VendorID: 111D

PCIe Retimer #9 VendorID: 111D

PCIe Retimer DeviceIDs

PCIe Retimer #1 DeviceID: 80E0

PCIe Retimer #2 DeviceID: 80E0

PCIe Retimer #3 DeviceID: 80E0

PCIe Retimer #4 DeviceID: 80E0

PCIe Retimer #5 DeviceID: 80E0

PCIe Retimer #6 DeviceID: 80E0

PCIe Retimer #7 DeviceID: 80E0

PCIe Retimer #8 DeviceID: 80E0

PCIe Retimer #9 DeviceID: 80E0

PCIe Retimer System Identifiers

PCIe Retimer #1 System Identifier: 00

PCIe Retimer #2 System Identifier: 00

PCIe Retimer #3 System Identifier: 00

PCIe Retimer #4 System Identifier: 00

PCIe Retimer #5 System Identifier: 00

PCIe Retimer #6 System Identifier: 00

PCIe Retimer #7 System Identifier: 00

PCIe Retimer #8 System Identifier: 00

PCIe Retimer #9 System Identifier: 00

PCIe Retimer Source Version

PCIe Retimer #1 Source Version: C385

PCIe Retimer #2 Source Version: C388

PCIe Retimer #3 Source Version: C386

PCIe Retimer #4 Source Version: C387

PCIe Retimer #5 Source Version: C381

PCIe Retimer #6 Source Version: C384

PCIe Retimer #7 Source Version: C382

PCIe Retimer #8 Source Version: C383

PCIe Retimer #9 Source Version: 199A

[HGX2 Baseboard(2)]

FPGA Image Version: 3.1

FPGA Loaded Image Index: 2

PEX8725 EEPROM Version: 1.6

Baseboard Revision: A02

Baseboard ID: 01

PCIe Retimer EEPROM Versions

PCIe Retimer #1 EEPROM Version: 2.0

PCIe Retimer #2 EEPROM Version: 2.0

PCIe Retimer #3 EEPROM Version: 2.0

PCIe Retimer #4 EEPROM Version: 2.0

PCIe Retimer #5 EEPROM Version: 2.0

PCIe Retimer #6 EEPROM Version: 2.0

PCIe Retimer #7 EEPROM Version: 2.0

PCIe Retimer #8 EEPROM Version: 2.0

PCIe Retimer #9 EEPROM Version: 2.0

PCIe Retimer VendorIDs

PCIe Retimer #1 VendorID: 111D

PCIe Retimer #2 VendorID: 111D

PCIe Retimer #3 VendorID: 111D

PCIe Retimer #4 VendorID: 111D

PCIe Retimer #5 VendorID: 111D

PCIe Retimer #6 VendorID: 111D

PCIe Retimer #7 VendorID: 111D

PCIe Retimer #8 VendorID: 111D

PCIe Retimer #9 VendorID: 111D

PCIe Retimer DeviceIDs

PCIe Retimer #1 DeviceID: 80E0

PCIe Retimer #2 DeviceID: 80E0

PCIe Retimer #3 DeviceID: 80E0

PCIe Retimer #4 DeviceID: 80E0

PCIe Retimer #5 DeviceID: 80E0

PCIe Retimer #6 DeviceID: 80E0

PCIe Retimer #7 DeviceID: 80E0

PCIe Retimer #8 DeviceID: 80E0

PCIe Retimer #9 DeviceID: 80E0

PCIe Retimer System Identifiers

PCIe Retimer #1 System Identifier: 00

PCIe Retimer #2 System Identifier: 00

PCIe Retimer #3 System Identifier: 00

PCIe Retimer #4 System Identifier: 00

PCIe Retimer #5 System Identifier: 00

PCIe Retimer #6 System Identifier: 00

PCIe Retimer #7 System Identifier: 00

PCIe Retimer #8 System Identifier: 00

PCIe Retimer #9 System Identifier: 00

PCIe Retimer Source Version

PCIe Retimer #1 Source Version: C385

PCIe Retimer #2 Source Version: C388

PCIe Retimer #3 Source Version: C386

PCIe Retimer #4 Source Version: C387

PCIe Retimer #5 Source Version: C381

PCIe Retimer #6 Source Version: C384

PCIe Retimer #7 Source Version: C382

PCIe Retimer #8 Source Version: C383

PCIe Retimer #9 Source Version: 199A

Notes:

- For more details on support, please refer to the following links.
  Supermicro - Qualified Platform List for NVIDIA vGPU
  NVIDIA vGPU
- The option--show_all is only supported by the HGX2 platform.

5.12 CPLD Management

5.12.1 Getting CPLD Firmware Image Information

Use the "GetCpldInfo" command to receive the CPLD firmware image information from the managed system as well as the local CPLD firmware image (with the option --file).

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
GetCpldInfo [--file <filename> [--file_only]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCpldInfo
```

The console output contains the following information.

```
Managed system.............192.168.34.56
    CPLD version..........F1.00.BD
    CPLD signed...........Signed
```

In-Band:

```
[SUM_HOME]# ./sum -c GetCpldInfo -I Redfish_HI -u ADMIN -p ADMIN --file CPLD.bin
```

The console output contains the following information.

```
Managed system...........localhost
    CPLD version.........F1.00.BD
    CPLD signed..........Signed
Local CPLD image file....CPLD.bin
    CPLD version.........F1.00.CD
    FW image.............Signed
         Signed Key.......RoT
```

An RoT-signed key of a local CPLD image displays the following information:

Type	Description
Signed	RoT is signed by Super Micro Computer, Inc.
Signed(U)	RoT is NOT signed by Super Micro Computer, Inc. but by an unknown authority.
Verification failed	The RoT signing in the image cannot be verified because the image is corrupted or incomplete.

Note: This command is only available on RoT systems of X12/H12 and later platforms.

5.12.2 Updating the CPLD Firmware Image

Use the command “UpdateCpld” with CPLD firmware image CPLD.bin to run SUM to update the CPLD of a managed system.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
UpdateCpld --file <filename> --reboot
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateCpld --file
CPLD.bin --reboot
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateCpld --file
CPLD.bin --reboot
```

Notes:

- This command is only available on RoT systems of X12/H12 and later platforms.
- System needs to be powered off while updating CPLD FW.

6 Managing Multiple Systems (OOB Only)

For managing multiple systems, SUM provides the "-l" option to concurrently execute OOB command on multiple systems enumerated in a system list file.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c <OOB command>
[command options]
```

The managed systems should be enumerated row-by-row in the system list file. Two formats are supported for general commands as follows. (For the ActivateProductKey command, different formats are used. Refer to *6.2.1 Activating Multiple Managed Systems*.)

```
Format 1: BMC_IP_or_HostName
Format 2: BMC_IP_or_HostName Username Password
```

Options -u and -p should be specified in the command line for Format 1. By contrast, options -u and -p can be removed from the command line for Format 2. In addition, the Username/Password in the system list file overwrites the options -u and -p in the command line.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt
--overwrite

SList.txt:
    192.168.34.56
    192.168.34.57 ADMIN1 PASSWORD1
```

For the first managed system 192.168.35.56, SUM applies -u ADMIN and -p PASSWORD in the command line to execute the GetDmiInfo command. On the other hand, for the second managed system 192.168.34.57, SUM adopts the username (ADMIN1) and password (PASSWORD1) in SList.txt to execute the GetDmiInfo command. Two executions are run concurrently and the execution status/results can be referenced in *6.1.2 File Output*, *6.1.3 Screen Output* and *6.1.4 Log Output*.

For the usage of commands that take input files as arguments, such as the UpdateBios command, see *6.1.1 File Input* for its usage.

Notes:

- Repeated managed system IPs or names in system list file are not allowed.
- SUM limits its maximum concurrent executing count to avoid system overloading. The default thread count in the .sumrc file is 50. For more details on usages, see *4.1 Customizing SUM Configurations*.

6.1 Input Output Controls for Multiple Systems

6.1.1 File Input

SUM uses the input file specified in the command line (through --file option) to manage multiple systems.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBios --file
SMCI_BIOS.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

In this example, SUM uses the input file SMCI_BIOS.rom specified in the command line to concurrently update BIOS for both managed systems 192.168.34.56 and 192.168.34.57 enumerated in the SList.txt file.

Note: SUM only supports single input files for managed systems in one command.

6.1.2 File Output

When SUM outputs files for managed systems, each managed system has one individual output file. The individual output file names are those specified in the command line (through --file option) appended by "." and the "BMC/CMM_IP_or_Hostname", which is obtained from the system list file.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt

SList.txt:
    192.168.34.56
    192.168.34.57
```

In this example, DMI information from the managed systems 192.168.34.56 and 192.168.34.57 is written to files “DMI.txt.192.168.34.56” and “DMI.txt.192.168.34.57”, respectively.

6.1.3 Screen Output

When SUM begins the execution for the managed systems, progress output will be continuously updated to a log file created when SUM is invoked.

When the SUM finishes execution, the final execution status for each managed system will be shown on the screen output row-by-row. Each row consists of “System Name”, “Elapsed”, “Status” and “Exit Code”. “System name” is the “BMC/CMM_IP_or_Hostname” from the system list file. “Elapsed” is the time elapsed when the command is executed. “Status” is provided as indicator: “WAITING”, “RUNNING”, “RETRY”, “SUCCESS”, or “FAILED.” The status summary will be shown before and after the status list. After listing the final status, SUM will exit and return the exit code of the concurrent executions.

You can also press the “ENTER” key to see the current execution status before the program is finished. The format of the current status is the same as the final status, but only shows the status of the managed systems at the stage of either “RUNNING” or “RETRY”. To see the current execution status of all managed systems, use the --show_multi_full option.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt
--overwrite

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt
--overwrite --show_multi_full

SList.txt:
    192.168.34.56
    192.168.34.57
```

Screen Output:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt
--overwrite
```

```
Supermicro Update Manager (for UEFI BIOS) 2.3.0 (2019/05/16) (x86_64)
Copyright(C)2019 Super Micro Computer, Inc. All rights reserved.
Start to do GetDmiInfo for systems listed in SList.txt
Multi system log file created:
  SList.txt.log_2019-04-11_15-50-43_5228
Press ENTER to see the current execution status:
---------------------------------Current Status---------------------------------
Executed Command:
  ./sum -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt --overwrite
Summary:
    3 EXECUTIONS (  WAITING: 0  RUNNING: 2  SUCCESS: 1  FAILED: 0  RETRY: 0  )
Status List:
         System Name |  Elapsed |     Status |  Exit Code
       10.136.160.26 | 00:00:03 |    RUNNING |
       10.136.160.27 | 00:00:03 |    RUNNING |
Summary:
    3 EXECUTIONS (  WAITING: 0  RUNNING: 2  SUCCESS: 1  FAILED: 0  RETRY: 0  )
--------------------------------------------------------------------------------


---------------------------------Final Results----------------------------------
Executed Command:
  ./sum -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt --overwrite
Summary:
    3 EXECUTIONS (  WAITING: 0  RUNNING: 0  SUCCESS: 3  FAILED: 0  RETRY: 0  )
Status List:
         System Name |  Elapsed |     Status |  Exit Code
       10.136.160.25 | 00:00:03 |    SUCCESS |          0
       10.136.160.26 | 00:00:05 |    SUCCESS |          0
       10.136.160.27 | 00:00:05 |    SUCCESS |          0
Summary:
    3 EXECUTIONS (  WAITING: 0  RUNNING: 0  SUCCESS: 3  FAILED: 0  RETRY: 0  )
```

```
--------------------------------------------------------------------------------


Please check SList.txt.log_2019-04-11_15-50-43_5228 for output message.


[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt
--overwrite --show_multi_full

Supermicro Update Manager (for UEFI BIOS) 2.3.0 (2019/05/16) (x86_64)
Copyright(C)2019 Super Micro Computer, Inc. All rights reserved.
Start to do GetDmiInfo for systems listed in SList.txt
Multi system log file created:
  SList.txt.log_2019-04-11_15-56-06_6563
Press ENTER to see the current execution status:
---------------------------------Current Status---------------------------------
Executed Command:
  ./sum -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt --overwrite
--show_multi_full
Summary:
    3 EXECUTIONS (  WAITING: 0  RUNNING: 2  SUCCESS: 1  FAILED: 0  RETRY: 0  )
Status List:
         System Name |  Elapsed |     Status |  Exit Code
       10.136.160.25 | 00:00:02 |    SUCCESS |           0
       10.136.160.26 | 00:00:03 |    RUNNING |
       10.136.160.27 | 00:00:03 |    RUNNING |
Summary:
    3 EXECUTIONS (  WAITING: 0  RUNNING: 2  SUCCESS: 1  FAILED: 0  RETRY: 0  )
--------------------------------------------------------------------------------

---------------------------------Final Results----------------------------------
Executed Command:
```

```
  ./sum -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt --overwrite
--show_multi_full
Summary:
    3 EXECUTIONS (  WAITING: 0  RUNNING: 0  SUCCESS: 3  FAILED: 0  RETRY: 0  )
Status List:
         System Name |  Elapsed |     Status |  Exit Code
       10.136.160.25 | 00:00:02 |    SUCCESS |           0
       10.136.160.26 | 00:00:05 |    SUCCESS |           0
       10.136.160.27 | 00:00:05 |    SUCCESS |           0
Summary:
    3 EXECUTIONS (  WAITING: 0  RUNNING: 0  SUCCESS: 3  FAILED: 0  RETRY: 0  )
--------------------------------------------------------------------------------


Please check SList.txt.log_2019-04-11_15-56-06_6563 for output message.
```

6.1.4 Log Output

When SUM is executed for the managed systems, a log file will be created. This log file will be continuously updated with the execution message for every system. The log file name, which will be shown on the screen, is the system list file name appended by ".log_", "yyyy-mm-dd_hh-mm-ss" (date and time) and "_PID" (process ID). The log file consists of one "Last Update Time" section, one "Execution parameters" section, one "Summary" section, one "Status List" section and, for each system, one "Execution Message" section. The following example shows the log file SList.txt.log_2013-10-02_15:57:40_7370 which was created from the example in *6.1.3 Screen Output*.

The SList.log will be saved in /var/log/supermicro/SUM if it exists. Otherwise, it will be saved in the same folder as SList.txt.

Example:

```
--------------------------------Last Update Time--------------------------------
2013-10-02_15:57:47
Process finished.
------------------------------Execution parameters------------------------------
IPMI server port: 38927
Executed Command:
  ./sum -l SList.txt -u ADMIN -p ***** -c GetDmiInfo --file DMI.txt --overwrite

-----------------------------------Summary------------------------------------
    2 EXECUTIONS (  WAITING: 0  RUNNING: 0  SUCCESS: 2  FAILED: 0  )

---------------------------------Status List----------------------------------
System Name       |Start Time     |End Time       |Elapsed |Status   |Exit Code
192.168.34.56     |10-02_15:57:40 |10-02_15:57:42 |00:00:02|SUCCESS  |0
192.168.34.57     |10-02_15:57:40 |10-02_15:57:47 |00:00:07|SUCCESS  |0

-------------------------------Execution Message------------------------------
System Name
    192.168.34.56
```

```
Message
Supermicro Update Manager (for UEFI BIOS) 1.2.0 (2013/10/02) Copyright (C) 2013
Super Micro Computer, Inc. All rights reserved

File "DMI.txt.192.168.34.56" is created.

--------------------------------Execution Message--------------------------------
System Name
    192.168.34.57
Message
Supermicro Update Manager (for UEFI BIOS) 1.2.0 (2013/10/02) Copyright (C) 2013
Super Micro Computer, Inc. All rights reserved

File "DMI.txt.192.168.34.57" is created.
```

6.2 Key Management for Multiple Systems

6.2.1 Activating Multiple Managed Systems

You can activate multiple systems concurrently using SUM through the -l option and the command "ActivateProductKey". (You should first obtain the node product keys for the managed systems. See *3.1 Receiving Node Product Keys from Supermicro*.)

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ActivateProductKey [--key_file <mymacs.txt.key>]
```

The managed systems should be enumerated row-by-row in the system list file. For the ActivateProductKey command, two formats are supported.

Format 1: BMC_IP_or_HostName Node_Product_Key

Format 2: BMC_IP_or_HostName Username Password Node_Product_Key

Options "-u" and "-p" options are required to specify in the command line for Format 1. The options -u and -p can be removed from the command line for Format 2. In addition, the Username/Password in the system list file overwrites the options -u and -p in the command line. If an option --key is specified in the command line, the exception will be thrown. If uses "--key_file" option you don't need apply Node_Product_Key in Format 1 or Format 2.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ActivateProductKey

SList.txt:
    192.168.34.56 1111-1111-1111-1111-1111-1111
    192.168.34.57 ADMIN1 PASSWORD1 2222-2222-2222-2222-2222-2222
```

```
    192.168.34.58 {"ProductKey":{"Node":{"LicenseID":"1","LicenseName":"SFT-OOB-
    LIC","CreateDate":"20200409"},"Signature":"11111111111111111112222222222222233333333
    33333333abababababababababababbabcdcdcdcdcdcdcdccdcdcddcdefefefefefefefefeefefefefghgh
    ghghghghghghghgh"}}

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ActivateProductKey --
key_file mymacs.text.key

SList.txt:
    192.168.34.56
    192.168.34.57 ADMIN1 PASSWORD1
```

For the first managed system 192.168.34.56, SUM applies -u ADMIN and -p PASSWORD to the command line and the node product key 1111-1111-1111-1111-1111-1111 to execute the command "ActivateProductKey". By contrast, for the second managed system 192.168.34.57, SUM adopts the username ADMIN1, password PASSWORD1 and node product key 2222-2222-2222-2222-2222-2222 to execute the command "ActivateProductKey". These two managed systems will be activated concurrently. The presentation of execution status and results will be similar to *6.1.3 Screen Output* and *6.1.4 Log Output*.

Note:

- For details on the command "ActivateProductKey," see the note in *5.1.1 Activating a Single Managed System.*

6.2.2 Querying Node Product Key

To query the node product keys activated in the managed systems, use the command "QueryProductKey".

Syntax:

```
sum -l < system list file > [-u <username> -p <password>] -c QueryProductKey
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c QueryProductKey
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field of a managed system is SUCCESS, the node product keys activated in the managed system will be shown in the “Execution Message” section in the created log file.

6.3 System Checks for Multiple System

6.3.1 Checking OOB Support

Use the command "CheckOOBSupport" to check if both BIOS and BMC firmware images support OOB functions for the managed systems. The received information will be the same as that in *5.2.1 Checking OOB Support (Single System)*.

Syntax:

```
sum -l < system list file > [-u <username> -p <password>] -c CheckOOBSupport
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c CheckOOBSupport

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the BIOS and BMC capabilities of the managed system will be shown in the "Execution Message" section in the created log file.

6.3.2 Checking Asset Information

Use the command "CheckAssetInfo" to check the asset information in the managed systems. The received information will be the same as that in *5.2.2 Checking Asset Information (OOB Only) (Single System)*.

Syntax:

```
sum -l < system list file > [-u <username> -p <password>] -c CheckAssetInfo
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c CheckAssetInfo
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the asset configuration of the managed system will be shown in the "Execution Message" section in the created log file.

6.3.3 Checking Sensor Data

Use the command "CheckSensorData" to check the sensor data of the managed systems. The message output will be the same as that in *5.2.3 Checking Sensor Data (OOB Only) (Single System)*.

Syntax:

```
sum -l < system list file > [-u <username> -p <password>] -c CheckSensorData
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c CheckSensorData

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the sensor data of the managed system will be shown in the "Execution Message" section in the created log file.

6.3.4 Checking System Utilization

Use the command "CheckSystemUtilization" to check the utilization status of the managed systems. The message output will be the same as that in *5.2.4 Checking System Utilization (OOB Only) (Single System)*.

Syntax:

```
sum -l < system list file > [-u <username> -p <password>] -c
CheckSystemUtilization
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c CheckSystemUtilization

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the utilization status of the managed system will be shown in the "Execution Message" section in the created log file.

6.3.5 ServiceCalls

Use the command "ServiceCalls" to check the system event log and sensor data record of the managed system with the ServiceCalls configuration file. After execution, you will receive the SEL and SDR report via e-mail. The message output will be the same as that in *5.2.5 ServiceCalls (Single System)*.

Syntax:

```
sum -l < system list file > [-u <username> -p <password>] -c ServiceCalls --file
<servicecalls XML file>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ServiceCalls --file
<servicecalls XML file>

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the utilization status of the managed system will be shown in the "Execution Message" section in the created log file.

6.4 BIOS Management for Multiple Systems

6.4.1 Getting BIOS Firmware Image Information

Use the command "GetBiosInfo" to receive the BIOS firmware image information from the managed systems as well as the input BIOS firmware image. The message output will be the same as that in *5.3.1 Getting BIOS Image Information (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBiosInfo [--file
<filename> [--showall]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBiosInfo --file
SMCI_BIOS.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

Note: If the execution "Status" field of a managed system is SUCCESS, the BIOS information of the managed system will be shown in its "Execution Message" section in the created log file.

6.4.2 Updating the BIOS Firmware Image

Use the command "UpdateBios" with the BIOS firmware image SMCI_BIOS.rom to update managed systems. For detailed usage notes of the "UpdateBios" command, see the usage notes in *5.3.2 Updating the BIOS Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateBios --file
<filename> [options…]
```

Option Commands	Descriptions
--reboot	Forces the managed systems to reboot.
--flash_smbios	Overwrites SMBIOS data.
--preserve_mer	Preserves ME firmware region.
--preserve_nv	Preserves NVRAM.
--preserve_setting	Preserves setting configurations.
--policy	Updates the BIOS based on the given policy file.
--backup	Backs up the current BIOS image. (Only supported by the RoT systems.)
--forward	Confirms the Rollback ID and upgrades to the next revision. (Only supported by the X12/H12 and later platforms except the H12 non-RoT systems.)

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBios --file
SMCI_BIOS.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

The execution progress for the managed system will be continuously updated to the “Execution Message” section of the managed system in the created log file.

6.4.3 Receiving Current BIOS Settings

Use the command “GetCurrentBiosCfg” to get the current BIOS settings from the managed systems and save it in the output files individually for each managed system enumerated in the system list file. For details on the command “GetCurrentBiosCfg”, see *5.3.3 Receiving Current BIOS Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetCurrentBiosCfg --
file <USER_SETUP.file> [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetCurrentBiosCfg --file
USER_SETUP.file --overwrite

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system (e.g. 192.168.34.56) is SUCCESS, its current settings are stored in its output file, e.g. USER_SETUP.file.192.168.34.56. The option --overwrite is used to force the overwrite of the existing file, e.g. USER_SETUP.file.192.168.34.56, if the output file already exists.

6.4.4 Updating BIOS Settings Based on a Current Sample Settings

1. Select one managed system as the golden sample for current BIOS settings.
2. Follow the steps in *5.3.3 Receiving Current BIOS Settings* for that system.
3. Edit the item/variable values in the user setup file USER_SETUP.file to the desired values as illustrated in *4.3 Format of BIOS Settings Text File* (for DAT) or *4.4 Format of BIOS Settings XML File* (for HII).
4. Remove unchanged items/variables in the text file. Note that this step is optional.
5. Use the command ChangeBiosCfg with the modified USER_SETUP.file to update the BIOS configurations for managed systems.

Notes:

- Use the --individually option to update each managed system with the corresponding configuration file.
- For details on the command "ChangeBiosCfg", see the note in *5.3.4 Updating BIOS Settings Based on the Current BIOS Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeBiosCfg --file
<USER_SETUP.file> [--reboot] [--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeBiosCfg --file
USER_SETUP.file --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeBiosCfg --file
USER_SETUP.file --reboot --individually

SList.txt:
    192.168.34.56
    192.168.34.57
```

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files USER_SETUP.file.192.168.34.56 and USER_SETUP.file.192.168.34.57. Then set the --file argument with the "USER_SETUP.file" file name. With the --individually option, SUM searches for USER_SETUP.file.192.168.34.56 and USER_SETUP.file.192.168.34.57 to update 192.168.34.56 and 192.168.34.57 respectively.

6.4.5 Receiving Factory BIOS Settings

Use the command "GetDefaultBiosCfg" to get the default factory BIOS settings from the managed systems and save it in the output files individually for each managed system enumerated in the system list file.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetDefaultBiosCfg --
file <USER_SETUP.file> [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetDefaultBiosCfg --file
USER_SETUP.file

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system (e.g. 192.168.34.56) is SUCCESS, its default settings are saved in its output file, e.g. USER_SETUP.file.192.168.34.56. The option --overwrite is used to force overwrite the existing file, e.g. USER_SETUP.file.192.168.34.56, if the output file already exists.

6.4.6 Updating BIOS Settings Based on Factory Sample Settings

1. Select one managed system as the golden sample for factory default BIOS settings.
2. Follow the steps in *5.3.5 Receiving Factory BIOS Settings* for that system.
3. Follow steps 3 to 5 in *6.4.4 Updating BIOS Settings Based on a Current Sample Settings*.

6.4.7 Loading Factory BIOS Settings

Use the command “LoadDefaultBiosCfg” to reset the BIOS settings of the managed systems to the factory default settings.

Note: The uploaded configurations will only take effect after the managed systems reboot or power up.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultBiosCfg [--reboot]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBiosCfg --reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

6.4.8 Receiving DMI Information

Use the command “GetDmiInfo” to get the current supported editable DMI information from the managed systems and save it in the output files individually for each managed system enumerated in the system list

file. For detailed usage notes of the command “GetDmiInfo”, see *5.3.8 Receiving DMI Information (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetDmiInfo --file
<DMI.txt>  [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt
--overwrite

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system (e.g. 192.168.34.56) is SUCCESS, its DMI settings are saved in its output file, e.g. DMI.txt.192.168.34.56. The option --overwrite is used to force overwrite of the existing file, e.g.DMI.txt.192.168.34.56.

6.4.9 Editing DMI Information

Use the command “EditDmiInfo” to edit the editable DMI items. For details on the “EditDmiInfo” command, refer to *5.3.9 Editing DMI Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c EditDmiInfo --file
<DMI.txt> --item_type <Item Type> --item_name <Item Name> --value <Item Value>

sum -l <system list file> [-u <username> -p <password>] -c EditDmiInfo --file
<DMI.txt> --shn <Item Short Name> --value <Item Value>

sum -l <system list file> [-u <username> -p <password>] -c EditDmiInfo --file
<DMI.txt> --shn <Item Short Name> --default
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --item_type "System" --item_name "Version" --value "1.01"

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --shn SYVS --value "1.01"

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --shn SYVS --default

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system (e.g. 192.168.34.56) is "SUCCESS", its edited DMI information are updated in its output file, e.g. DMI.txt.192.168.34.56.

6.4.10 Updating DMI Information Based on a Sample DMI Information

1. Select one managed system as the golden sample for DMI information.
2. Follow the steps in *5.3.9 Editing DMI Information* to prepare the edited DMI.txt file for updating DMI information.
3. Use the command "ChangeDmiInfo" with the edited DMI.txt file to update the DMI information for the managed systems.

Notes:

- The uploaded information will only take effect after the managed systems reboot or power up.
- Use the --individually option to update each managed system with the corresponding configuration filey.
- For detailed usage notes of the command "ChangeDmiInfo", see *5.3.10 Updating DMI Information*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeDmiInfo --file
<DMI.txt>  [--reboot] [--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeDmiInfo --file
DMI.txt --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeDmiInfo --file
DMI.txt --reboot --individually

SList.txt:
    192.168.34.56
    192.168.34.57
```

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files DMI.txt.192.168.34.56 and DMI.txt.192.168.34.57. Then set the --file argument with the DMI.txt" file name. With the --individually option, SUM searches for DMI.txt.192.168.34.56 and DMI.txt.192.168.34.57 to update 192.168.34.56 and 192.168.34.57 respectively.

6.4.11 Setting BIOS Action

Use the command “SetBiosAction” to show or hide BBS priority related settings.

Note: The uploaded configurations will only take effect after the managed systems reboot or power up.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetBiosAction --BBS
<yes/no> [--reboot]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBiosAction --BBS yes
--reboot
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.4.12 Setting BIOS Administrator Password

Use the command “SetBiosPassword” to update a BIOS Administrator password.

Note: The new uploaded password will only take effect after the managed systems reboot or power up.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetBiosPassword
[[--new_password <new password> --confirm_password <confirm password>] | [--
pw_file <password file path>]] [--reboot]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBiosPassword
--new_password 123456 --confirm_password 123456 --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBiosPassword
--pw_file passwd.txt --reboot

SList.txt:
    192.168.34.56
    192.168.34.57

passwd.txt:

    BiosPassword
```

6.4.13 Managing BIOS RoT Funtions

Use the command “BiosRotManage” to manage RoT fuctions. For details, see *5.3.14 Managing BIOS RoT Functions (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c BiosRotManage --
action <action> [--reboot]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c BiosRotManage --action
UpdateGolden --reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

6.5 BMC Management for Multiple Systems

6.5.1 Getting BMC Firmware Image Information

Use the command “GetBmcInfo” to receive the BMC firmware image information from the managed systems as well as the input BMC firmware image. The information will be the same as that in *5.4.1 Getting BMC Image Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBmcInfo [--file
<filename>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBmcInfo --file
SMCI_BMC.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution ”Status” field for a managed system is SUCCESS, the BMC information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.5.2 Updating the BMC Firmware Image

Use the command “UpdateBmc” with BMC firmware image SMCI_BMC.rom to update managed systems. For detailed usage notes of the “UpdateBmc” command, see the usage notes in *5.4.2 Updating the BMC Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateBmc --file
<filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--
overwrite_ssl]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBmc --file
SMCI_BMC.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

The execution progress for the managed system will be continuously updated to the "Execution Message" section of the managed system in the created log file.

6.5.3 Receiving BMC Settings

Use the command "GetBmcCfg" to get the current BMC settings from the managed systems and save it in the output files individually for each managed system enumerated in the system list file. For detailed usage notes of the "GetBmcCfg" command, see the usage notes in *5.4.3 Receiving BMC Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBmcCfg --file <
BMCCfg.xml > [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBmcCfg --file
BMCCfg.xml --overwrite

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system (e.g. 192.168.34.56) is SUCCESS, its current settings will be stored in its output file, e.g. BMCCfg.xml.192.168.34.56. The option --overwrite is used to force the overwrite the existing file, e.g. BMCCfg.xml.192.168.34.56.

6.5.4 Updating BMC Settings

1. Select one managed system as the golden sample for current BMC settings.
2. Follow the steps in *5.4.3 Receiving BMC Settings* for the managed system.
3. Edit the configurable element values in the BMC configuration text file BMCCfg.xml to the desired values as illustrated in *4.6 Format of BMC Configuration Text File*.
4. Skip unchanged tables in the text file by setting Action attribute as "None". Note that this step is optional.
5. Remove unchanged tables/elements in the text file. Note that this step is optional.
6. Use the command "ChangeBmcCfg" with the modified BMCCfg.xml file to update the BMC configurations for multiple systems.

Notes:

- Some table settings cannot be applied to each managed system uniformly, e.g., FRU and LAN configurations. You might need to change its table action to "None" in step 4 or remove tables/elements in step 5.
- LAN "*IPAddress*" field will be skipped in multiple system usage.
- Use the --individually option to update each managed system with the corresponding configuration file.
- For detailed usage notes of the "ChangeBmcCfg" command, see the usage notes in *5.4.4 Updating BMC Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeBmcCfg --file
<BMCCfg.xml> [--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcCfg --file
BMCCfg.xml

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcCfg --file
BMCCfg.xml --individually
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, its BMC settings are updated.

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files BMCCfg.xml.192.168.34.56 and BMCCfg.xml.192.168.34.57. Then set the argument --file with the BMCCfg.xml file name. With the option --individually, SUM searches for BMCCfg.xml.192.168.34.56 and BMCCfg.xml.192.168.34.57 to update 192.168.34.56 and 192.168.34.57 respectively.

6.5.5 Setting Up the BMC User Password

Use the command "SetBmcPassword" to execute SUM to update the BMC user password. The information will be the same as that in *5.4.6 Setting Up a BMC User Password (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetBmcPassword [--
user_id <user ID>] [[--new_password <new password> --confirm_password <confirm
password>] | [--pw_file <password file path>]]
```

The managed systems should be enumerated row by row in the system list file. For the "SetBmcPassword" command, two formats are supported.

Format 1: BMC_IP_or_HostName New_Password

Format 2: BMC_IP_or_HostName Username Password New_Password

The "-u" and "-p" options are required to specify in the command line for Format 1. The options "-u" and "-p" can be removed from the command line for Format 2. In addition, the Username/Password in the system list file overwrites the options "-u" and "-p" in the command line. When using either the "--new_password" or "--pw_file" options, you don't need to include New_Password for Format 1 or Format 2, and the same new password will apply to each system specified in the system list file. If you want to set a different new password for each system, you can specify a New_Password corresponding to each system for Format 1 or Format 2 without using the "--new_password" and "--pw_file" options.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBmcPassword

SList.txt:
    192.168.34.56 12345678
    192.168.34.57 ADMIN1 PASSWORD1 87654321

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBmcPassword
--new_password 12345678 --confirm_password 12345678
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBmcPassword
--user_id 3 --pw_file passwd.txt

SList.txt:
    192.168.34.56
    192.168.34.57

passwd.txt:

    BmcPasswordString
```

6.5.6 Receiving the BMC KCS Privilege Level

Use the command "GetKcsPriv" to execute SUM to get the current BMC KCS privilege level from the managed systems.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetKcsPriv
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetKcsPriv
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.5.7 Setting the BMC KCS Privilege Level

Use the command "SetKcsPriv" to execute SUM to set the BMC KCS privilege level. The information will be the same as that in *5.4.8 Setting the BMC KCS Privilege Level (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetKcsPriv
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetKcsPriv --privi_level
'Call Back'
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetKcsPriv --privi_level
1
```

SList.txt:

192.168.34.56

192.168.34.57

6.5.8 Loading Factory BMC Settings

Use the command “LoadDefaultBmcCfg” to execute SUM to reset the BMC of the managed system to the factory default. For details, see *5.4.9 Loading Factory BMC Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultBmcCfg --
preserve_user_cfg

sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultBmcCfg --
clear_user_cfg --load_unique_password

sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultBmcCfg --
clear_user_cfg --load_default_password
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg --
preserve_user_cfg

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg --
clear_user_cfg --load_unique_password

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg --
clear_user_cfg --load_default_password

SList.txt:
    192.168.34.56
    192.168.34.57
```

6.5.9 Acquiring the BMC System Lockdown Mode Status

Use the command "GetLockdownMode" to execute SUM to get the current BMC system lockdown mode status of the managed systems.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetLockdownMode
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetLockdownMode
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.5.10 Setting the BMC System Lockdown Mode

Use the command "SetLockdownMode" to execute SUM to set the BMC system lockdown mode. For details, see *5.4.10 Setting the BMC System Lockdown Mode (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetLockdownMode --
lock <yes/no> --reboot
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetLockdownMode --lock
<yes/no> --reboot
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.5.11 Managing BMC RoT Functions

Use the command “BmcRotManage” to manage RoT functios. For details, see *5.4.11 Managing BMC RoT Functions (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c BmcRotManage --action
<action>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c BmcRotManage --action
UpdateGolden
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.5.12 Setting the BMC Reset Counter

To set the BMC reset counter, use the “TimedBmcReset” command. For details, see *5.3.13 Setting the BMC Reset Counter*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c TimedBmcReset --dalay
< BMC reset delay time>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TimedBmcReset --delay 10
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.6 Event Log Management for Multiple Systems

6.6.1 Getting System Event Log

Use the command “GetEventLog” to show the current system event log (including both BIOS and BMC event log) from the managed systems and save them in the output files individually for each managed system enumerated in the system list file with the --file option. Without --file option, you can choose to show the event log in the execution log file instead. For detailed execution notes, see *5.5.1 Getting System Event Log (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetEventLog [--file
<EventLog.txt>] [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetEventLog --file
EventLog.txt

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system (e.g. 192.168.34.56) is SUCCESS, its event logs are stored in its output file, e.g. EventLog.txt.192.168.34.56. The option --overwrite is used to force overwrite of the existing file, e.g. EventLog.txt.192.168.34.56. If --file option is not used, the event log for each managed system will be shown in the “Execution Message” section of the managed system in the created execution log file.

6.6.2 Clearing System Event Log

Use the command “ClearEventLog” to clear the event log (both BMC and BIOS event log) for each managed system. For detailed execution notes, see *5.5.2 Clearing System Event Log (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ClearEventLog [--
reboot]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ClearEventLog --reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, its event logs are cleared.

6.6.3 Getting the System Maintenance Event Log

Use the command "GetMaintenEventLog" to have SUM show the managed system's current maintenance event logs (including both BIOS and BMC event logs), and use the option --file to save them in the output files separately. Without the option --file, you can show the event log in the execution log file instead. For details, see *5.5.3 Getting System Maintenance Event Log (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetMaintenEventLog –
st <start time> --et <end time> [--count <log count>]  [--file
<MaintenanceEventLog.txt>] [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetMaintenEventLog --st
20200601 --et 20200610 --count 10 --file EventLog.txt
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the "Status" field of the managed system (e.g. 192.168.34.56) shows SUCCESS, its maintenance event logs are stored in its output file, e.g., MaintenanceEventLog.txt.192.168.34.56. The option --overwrite is used to force to overwrite the existing file, e.g., MaintenanceEventLog.txt.192.168.34.56. If the option --file is not used, the event logs of each managed system will be shown in its "Execution Message" section in the created execution log file.

6.6.4 Getting Host Crash Dump Data Log

Use the command "GetHostDump" to have SUM show the managed system's host crash dump data logs. For details, see *5.5.4 Getting Host Crash Dump Log (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetHostDump --action
<actiondump> [--file <HostDump.tgz>] [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetHostDump --action
DeleteDump

SList.txt:
    192.168.34.56
    192.168.34.57
```

6.6.5 Clearing System Maintenance Event Log

Use the command “ClearMaintenEventLog” to clear the maintenance event log for each managed system. For details, see *5.5.5 Clearing System Maintenance Event Log (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ClearMaintenEventLog
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ClearMaintenEventLog

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, its maintenance event logs are cleared.

6.7 CMM Management for Multiple Systems

The CMM provides total remote control of individual blade server nodes, power supplies, power fans, and networking switches. The controller is a separate processor, allowing all monitoring and control functions operate flawlessly regardless of CPU operation or system power-on status.

Note: Three models of 7U SuperBlade CMMs, including SBM-CMM-001, BMB-CMM-002 (mini-CMM) and SBM-CMM-003 are no longer supported.

6.7.1 Receiving CMM Image Information

Use the command "GetCmmInfo" to receive the CMM firmware image from the managed systems as well as the input CMM firmware image. The information will be the same as that in *5.6.1 Receiving CMM Firmware Image Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetCmmInfo [--file
<filename>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetCmmInfo --file
SMCI_CMM.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the Status field for a managed system shows "SUCCESS", the CMM information of the managed system will be shown in the "Execution Message" section of the managed system in the created log file.

6.7.2 Updating the CMM Firmware Image

Use the command "UpdateCmm" with the CMM firmware image SMCI_CMM.rom to update managed systems. For details on the "UpdateCmm" command, see the notes in *5.6.2 Updating the CMM Firmware Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateCmm --file
<filename> [--overwrite_cfg] [--overwrite_sdr] [--overwrite_ssl]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateCmm --file
SMCI_CMM.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

The execution progress of the system will be continuously updated in the "Execution Message" section of the managed system in the created log file.

6.7.3 Receiving CMM Settings

Use the command "GetCmmCfg" to get the current CMM settings from managed systems and save it in the output files individually for each managed system enumerated in the system list file. For details on the "GetCmmCfg" command, see the notes in *5.6.3 Receiving CMM Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetCmmCfg --file <
CMMCfg.xml > [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetCmmCfg --file
CMMCfg.xml --overwrite
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the Status field of the managed system (e.g. 192.168.34.56) shows SUCCESS, its current settings are stored in its output file, e.g. CMMCfg.xml.192.168.34.56. The option --overwrite is used to force the overwrite of the existing file, e.g. CMMCfg.xml.192.168.34.56.

6.7.4 Updating CMM Settings

1. Select one managed system as the golden sample for the current CMM settings.
2. Follow the steps in *5.6.3 Receiving CMM settings*.
3. Edit the configurable element values in the CMM configuration text file CMMCfg.xml to the desired values as illustrated in *4.8 Format of CMM Configuration Text File*.
4. Set the Action attribute as "None" to skip unchanged tables in the text file. Note that this step is optional.
5. Remove unchanged tables/elements in the text file. Note that this step is optional.
6. Use the command "ChangeCmmCfg" with the modified CMMCfg.xml file to update the CMM configurations for multiple systems.

Notes:

- Some table settings cannot be applied to each managed system uniformly, e.g., LAN configurations. You might need to change its table action to "None" in step 4 or remove tables/elements in step 5.
- LAN "*IPAddress*" field will be skipped in multiple system usage.
- Use the --individually option to update each managed system with the corresponding configuration file.
- For details on the "ChangeCmmCfg" command, see the notes in *5.6.4 Updating CMM Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeCmmCfg --file
<CMMCfg.xml> [--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeCmmCfg --file
CMMCfg.xml

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeCmmCfg --file
CMMCfg.xml --individually

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the Status field of a managed system shows “SUCCESS”, its CMM settings are updated.

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files CMMCfg.xml.192.168.34.56 and CMMCfg.xml.192.168.34.57. Then set the --file argument with CMMCfg.xml” file name. With the --individually option, SUM searches for CMMCfg.xml.192.168.34.56 and CMMCfg.xml.192.168.34.57 to update 192.168.34.56 and 192.168.34.57 respectively.

6.7.5 Setting Up a CMM User Password

Use the command “SetCmmPassword” to execute SUM to update a CMM user password.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetCmmPassword [--
user_id <user ID>] [[--new_password <new password> --confirm_password <confirm
password>] | [--pw_file <password file path>]]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetCmmPassword
--new_password 12345678 --confirm_password 12345678

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetCmmPassword
--user_id 3 --pw_file passwd.txt

SList.txt:
    192.168.34.56
    192.168.34.57
```

```
passwd.txt:

    CmmPasswordString
```

6.7.6 Loading Factory CMM Settings

Use the command "LoadDefaultCmmCfg" to have SUM reset the CMM of the managed system to the factory default. For details, see *5.6.6 Loading Factory CMM Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultCmmCfg --
preserve_user_cfg

sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultCmmCfg --
clear_user_cfg --load_unique_password

sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultCmmCfg --
clear_user_cfg --load_default_password
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultCmmCfg --
preserve_user_cfg

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultCmmCfg --
clear_user_cfg --load_unique_password

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultCmmCfg --
clear_user_cfg --load_default_password

SList.txt:
    192.168.34.56
    192.168.34.57
```

6.7.7 Receiving BBP Image Information

Use the command “GetBbpInfo” to receive the BBP firmware image from the managed systems as well as the input BBP firmware image. The information will be the same as that in *5.6.7 Receiving BBP Firmware Image Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBbpInfo [--file
<filename>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBbpInfo --file BBP.bin

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the Status field for a managed system shows “SUCCESS”, the BBP information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.7.8 Updating the BBP Firmware Image

Use the command “UpdateBbp” with the BBP firmware image BBP.bin to update managed systems. For details on the command “UpdateBbp”, see the notes in *5.6.8 Updating the BBP Firmware Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateBbp --file
<filename> [--skip_check]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBbp --file BBP.bin
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

The execution progress of the system will be continuously updated in the “Execution Message” section of the managed system in the created log file.

6.7.9 Getting Current Power Status of Blade System

Use the command “GetBladePowerStatus” to get the current power status of the blade system. See *5.5.9 Getting Current Power Status of Blade System (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBladePowerStatus
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBladePowerStatus

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the Status field for a managed system shows “SUCCESS”, the power status of the blade system will be shown in the “Execution Message” section of the managed system in the created log file.

6.7.10 Setting Power Status of Blade System

Use the command “SetBladePowerAction” to set the current power status of the blade system. See *5.5.10 Setting Power Status of Blade System (Single System)*.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetBladePowerAction --
action <action> --blade <Blade Index> [--node <Node Index>]
```

Option Commands	Descriptions
--action (optional)	Sets power action with: 0 = down 1 = up 2 = cycle 3 = reset 4 = accycle 5 = softshutdown
--blade	Sets blade index. [A1-A14], [B1-B14] or "ALL"
--node (optional)	Sets node index.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBladePowerAction
--action down --blade ALL

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBladePowerAction
--blade ALL --action reset

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBladePowerAction
--blade A1 --node 1 --action softshutdown

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the console output of the managed system will be shown in the "Execution Message" section of the managed system in the created log file.

6.8 Applications for Multiple Systems

6.8.1 Providing an ISO Image as a Virtual Media through BMC and File Server

Use the command “MountIsoImage” to mount ISO image as a virtual media to managed systems through SAMBA/HTTP server. For detailed “MountIsoImage” command notes, see *5.7.1 Providing an ISO Image as a Virtual Media through BMC and File Server (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c MountIsoImage --
image_url <URL> --reboot [[--id <id for URL> --pw <password for URL>] | [--id
<id for URL> --pw_file <password file path>]]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --image_url
'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --image_url
'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --image_url
'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --image_url
'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpassw

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --image_url
'\\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id smbid --pw_file
smbpasswd.txt

SList.txt:
    192.168.34.56
```

```
    192.168.34.57

smbpasswd.txt:
smbpasswd
```

If the execution “Status” field for a managed system is SUCCESS, the Image.iso is mounted as a virtual media to the managed system.

6.8.2 Removing ISO Image as a Virtual Media

Use the command “UnmountIsoImage” to unmount an ISO image as a virtual media from managed system.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UnmountIsoImage
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UnmountIsoImage

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the mounted virtual media will be removed from the managed system.

6.8.3 Mounting a Floppy Image as Virtually from a Local Image File

Use the command “MountFloppyImage” to execute SUM to mount a binary floppy image virtuallyto the managed system. For details on “MountFloppyImage”, see *5.7.3 Mounting a Floppy Image Virtually from a Local Image File (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c MountFloppyImage

--file <filename>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountFloppyImage --file
Floppy.img

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field of the managed system is SUCCESS, the “Floppy.img” is mounted virtually to the managed system.

6.8.4 Unmounting a Floppy Image as Virtually from the Managed System

Use the command “UnmountFloppyImage” to remove a binary floppy image virtually from the managed system. For details on “UnmountFloppyImage”, see *5.7.4 Unmounting Floppy Image Virtually from the Managed System (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UnmountFloppyImage
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UnmountFloppyImage

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the virtually mounted image will be removed from the managed system.

6.8.5 Sending an IPMI Raw Command

Use the command “RawCommand” to send IPMI raw command.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c RawCommand --raw
<raw command>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c RawCommand --raw '06 01'

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c RawCommand --raw '0x6
0x01'

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the console output of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

Note: A raw command has to be quoted.

6.8.6 Controlling the UIDs of Multiple Managed Systems

Use the command “LocateServerUid” to control the UIDs. For details, see *5.7.9 Controlling the UID of the Managed System (Single System)*.

Option Command	Description
--action	Sets action to: 1 = GetStatus 2 = On 3 = Off

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c LocateServerUid –
action <action>
```

Example:

```
[SUM_HOME]# ./sum –l SList.txt -u ADMIN -p PASSWORD -c LocateServerUid --action
3

[SUM_HOME]# ./sum –l SList.txt -u ADMIN -p PASSWORD -c LocateServerUid --action
GetStatusSList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the console output of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.8.7 Booting into the ISO Image from HTTP Server

Use the command "SetHttpBoot" to download ISO images from multiple servers and boot into the ISO image. For details, see *5.7.10 Booting into the ISO Image from HTTP Server (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetHttpBoot [--
boot_lan <boot lan port>] [--boot_name <boot description>] --image_url <URL> [--
reboot]

sum -l <system list file> [-u <username> -p <password>] -c SetHttpBoot --
boot_clean [--reboot]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetHttpBoot --boot_lan 1
--boot_name bootDescription --image_url http://192.168.12.78/iso/boot.iso --
reboot

[SUM_HOME]# ./sum -i SList.txt -u ADMIN -p PASSWORD -c SetHttpBoot --boot_lan 2
--boot_name bootDescription --image_url
https://[1234:ab5:0:c678:9012:345d:6e78:9f0a]/iso/boot.iso --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetHttpBoot --boot_clean
--reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the console output of the managed system will be shown in the "Execution Message" section of the managed system in the created log file.

Notes:

- HTTPS boot needs to provide the clients with a valid TLS certificate signed by a trusted certification authority. Please use the "ChangeBiosCfg" command to upload the TLS certificate, see *E.5.1 File Upload*.
- Due to BIOS limitations, if an HTTP boot option exists in the BIOS configuration, please use the option "--boot_clean" to clean the HTTP boot option and then reset HTTP the boot option.

6.9 Storage Management for Multiple Systems

6.9.1 Getting RAID Firmware Image Information

Use the command "GetRaidControllerInfo" to receive the RAID firmware image information from the managed systems as well as the input RAID firmware image. The information will be the same as that in *5.8.1 Getting RAID Firmware Image Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetRaidControllerInfo
[--controller <Broadom or Marvell>] [--dev_id <controller_id>] [--file
<filename>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetRaidControllerInfo --
file RAID.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the RAID information of the managed system will be shown in the "Execution Message" section of the managed system in the created log file.

6.9.2 Updating the RAID Firmware Image

Use the command "UpdateRaidController" with the RAID firmware image RAID.rom to update multiple systems. For details on using the "UpdateRaidController" command, see the usage notes in *5.8.2 Updating the RAID Firmware Image (OOB Only) (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateRaidController
--controller <Broadom or Marvell> --dev_id <controller_id> --file <filename>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateRaidController

--controller Broadcom --dev_id 0 --file SMCI_RAID.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

The execution progress for the managed system will be continuously updated in the "Execution Message" section of the managed system in the created log file.

6.9.3 Receiving RAID Settings

Use the command "GetRaidCfg" to get the current RAID settings from managed systems and save them separately for each managed system enumerated in the system list file. For details on using the "GetRaidCfg" command, see the usage notes in *5.8.3 Receiving RAID Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetRaidCfg --file <
RAIDCfg.xml > [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetRaidCfg --file
RAIDCfg.xml --overwrite

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system (e.g. 192.168.34.56) is SUCCESS, its current settings are stored in its output file, e.g. RAIDCfg.xml.192.168.34.56. The option --overwrite is used to force the overwrite of the existing file, e.g. RAIDCfg.xml.192.168.34.56.

6.9.4 Updating RAID Settings

1. Select one managed system as the golden sample for current RAID settings.
2. Follow the steps in *5.8.3 Receiving RAID Settings*.
3. Edit the configurable element values in the RAID configuration text file RAIDCfg.xml as illustrated in *4.7 Format of the RAID Configuration Text File*.
4. Set Action attribute as "None" to skip the unchanged tables in the text file. Note that this step is optional.
5. Remove the unchanged tables/elements in the text file. Note that this step is optional.
6. Use the command "Chang eRaidCfg" with the modified RAIDCfg.xml file to update the RAID configurations for multiple systems.

Notes:

- Some table settings cannot be uniformly applied to each managed system. You might need to change its table action to "None" in step 4 or remove the tables/elements in step 5.
- Use the "--individually" option to update each managed system with the corresponding configuration file concurrently.
- For details on the "ChangeRaidCfg" command, see the usage notes in *5.8.4 Updating RAID Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeRaidCfg --file
<RAIDCfg.xml> [--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeRaidCfg --file
RAIDCfg.xml

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeRaidCfg --file
RAIDCfg.xml --individually

SList.txt:
    192.168.34.56
```

```
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, its RAID settings are updated.

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files RAIDCfg.xml.192.168.34.56 and RAIDCfg.xml.192.168.34.57. Then set the --file argument with RAIDCfg.xml” file name. With the “--individually” option, SUM searches for RAIDCfg.xml.192.168.34.56 and RAIDCfg.xml.192.168.34.57 to update 192.168.34.56 and 192.168.34.57 respectively.

6.9.5 Getting SATA HDD Information

Use the command “GetSataInfo” to receive the SATA HDD information from the managed systems. The information will be the same as that in *5.8.5 Getting SATA HDD Information (OOB Only) (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetSataInfo
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetSataInfo

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the SATA HDD information of the managed system will be shown in the console.

6.9.6 Getting NVMe Information

Use the command "GetNvmeInfo" to receive the NVMe information from managed systems. The information will be the same as that in *5.8.6 Getting NVMe Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetNvmeInfo [ --
dev_id <device_id> ]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetNvmeInfo

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the NVMe information of the managed system will be shown on the console.

6.9.7 Securely-Erasing Hard Disks

Use the command “SecureEraseDisk” to execute SUM to erase the HDD on the managed system. For details, see *5.8.7 Secure Erasing Hard Disks (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SecureEraseDisk --
file <filename> [--action <action> --reboot] [--precheck]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseDisk --file
psid.txt --precheck

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseDisk --file
psid.txt --action SetPassword --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseDisk --file
psid.txt --action SecurityErase --reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution ”Status” field of a managed system is SUCCESS, the pre-check result of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.9.8 Securely Erasing Hard Disks in LSI MegaRaid SAS 3108 RAID Controller

Use the command “SecureEraseRaidHdd” to execute SUM to securely erase hard disks (HDD or SSD) in the target LSI MegaRaid SAS 3108 storage controller system and poll the erasing status asynchronously or synchronously. For details, see *5.8.8 Secure Erasing Hard Disks in LSI MegaRaid SAS 3108 RAID Controller (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SecureEraseRaidHdd

--dev_id <device_id> --enc_id <enclosure id> --dsk_id <disk id>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD –c SecureEraseRaidHdd

--dev_id 0 --enc_id 0,1,2 --dsk_id 0,3,4

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD –c SecureEraseRaidHdd

--dev_id 0 --enc_id ALL --dsk_id ALL

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution ”Status” field of a managed system is SUCCESS, the summary of securely erasing result of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

Note: In multiple systems, the synchronous mode is not supported. The --sync option is not allowed to erase disk(s) on the LSI MegaRaid SAS 3108 RAID controller system.

To check the erasing status, get the task ID(s) existing in the log file created from securely erasing and use the command “SecureEraseRaidHdd” appended with --tsk_id option.

Syntax:

```
[SUM_HOME]# ./sum -l <system list file> -u ADMIN -p PASSWORD –c
SecureEraseRaidHdd

--tsk_id <task id>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt –u ADMIN -p PASSWORD –c SecureEraseRaidHdd

--tsk_id 1,2,3
```

If the execution ”Status” field for a managed system shows SUCCESS, the erasing status of the LSI MegaRaid SAS 3108 RAID Controller systems will be shown in the “Execution Message” section of the managed system in the created log file.

6.9.9 Getting PMem Firmware Image Information

Use the command “GetPMemInfo” to receive the PMem firmware image information from the managed system as well as the input PMem firmware image. For details, see *5.8.9 Getting PMem Firmware Image Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetPMemInfo [--file
<filename>]
```

```
Example:
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetPMemInfo --file
PMem.bin
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution ”Status” field for a managed system is SUCCESS, the BMC information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.9.10 Updating the PMem Firmware Image

Use the command “UpdatePMem” with a PMem firmware image PMem.bin to update the PMem of the managed systems. For details on the command, see notes in *5.8.10 Updating the PMem Firmware Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdatePMem [[--file
<filename>] | [--restore_default_fw]] [--reboot]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdatePMem –file PMem.bin
--reboot
```

SList.txt:

```
    192.168.34.56
    192.168.34.57
```

The execution progress for the managed system will be continuously updated to the “Execution Message” section of the managed system in the created log file.

6.10 PSU Management for Multiple Systems

6.10.1 Getting PSU Information

Use the command “GetPsuInfo” to get the current PSU information from the managed systems. The PSU information output will be the same as that in *5.9.1 Getting PSU Information (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetPsuInfo
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetPsuInfo

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the PSU information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.10.2 Updating the Signed PSU Firmware Image Requested by OEM

Use the command “UpdatePsu” with a signed PSU firmware image requested by OEM and PSU slave address to run SUM to update the managed systems. For details on the UpdatePsu command, see the notes in *5.9.2 Updating the Signed PSU Firmware Image Requested by OEM (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdatePsu --file
<filename> --address <PSU slave address>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdatePsu --file
SMCI_PSU.x0 --address 0x80
```

The execution progress for the managed system will be continuously updated to the “Execution Message” section of the managed system in the created log file.

Note: To use “UpdatePsu” command for multiple systems, the slave addresses of PSUs that need to be updated must be the same.

6.10.3 Getting the Current Power Status of the Managed System

Use the command “GetPowerStatus” to get current power status of the managed system.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetPowerStatus
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetPowerStatus

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the console output of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.10.4 Setting Power Action of Managed System

Use the command “SetPowerAction” to set the type of power action of the managed system.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetPowerAction --
action <action>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetPowerAction --action
up

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetPowerAction --action 0

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the console output of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.11 TPM Management for Multiple Systems

6.11.1 Getting TPM Information

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the command "GetTpmInfo" to receive the TPM module information from the managed system. For detailed usage notes of the "GetTpmInfo" command, see the usage notes in *5.10.1 Getting TPM Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>]-c GetTpmInfo [--showall]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetTpmInfo [--showall]

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the TPM module information of the managed system will be shown in the "Execution Message" section of the managed system in the created log file.

6.11.2 Provisioning TPM Module

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the command "TpmManage" to execute SUM to enable TPM module capabilities for the managed system. Before executing the command, the TPM module should be installed on the managed system. For detailed usage notes of the "TpmManage" command, see the usage notes in *5.10.2 Provisioning TPM Module (Single System)*.

Option Commands	Descriptions
--reboot	Forces the managed system to reboot.
--provision	Launches the trusted platform module provision procedure.
--table_default	Uses the default TPM provision table.
--table <file name>	Uses the customized TPM provision table.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c TpmManage --image
provision [options…]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmManage -- provision
--table_default --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmManage -- provision
--table Tpm12Prov.bin --reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the TPM provisioning procedure is completed.

On platforms before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, use the command "TpmProvision" to enable TPM module capabilities for managed systems. Before executing the

command, the TPM modules should be installed on managed systems. For detailed notes of the "TpmProvision" command, see *5.10.2 Provisioning TPM Module (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>]-c TpmProvision --
image_url <URL> --reboot --lock <yes> [[--id <id for URL> --pw <password for
URL>] | [--id <id for URL> --pw_file <password file path>]]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmProvision --image_url
'smb://192.168.35.1/MySharedPoint/MyFolder/' --id smbid --pw smbpasswd --reboot
--lock yes

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmProvision --image_url
'http://192.168.35.1/MySharedPoint/MyFolder/' --id smbid --pw smbpasswd --reboot
--lock yes

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmProvision --image_url
'\\192.168.35.1\MySharedPoint\MyFolder\' --id smbid --pw_file smbpasswd.txt --
reboot --lock yes

SList.txt:
    192.168.34.56
    192.168.34.57

smbpasswd.txt:
smbpasswd
```

If the execution "Status" field for a managed system is SUCCESS, its TPM capabilities are enabled.

6.11.3 Enabling and Clearing TPM Module Capabilities

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the command "TpmManage" with the options in the following table to provide TPM module capabilities from the managed system. For detailed usage notes, see the usage notes in *5.10.3 Enabling and Clearing TPM Module Capabilities (Single System)*.

Option Commands	Descriptions
--reboot (optional)	Forces the managed system to reboot.
--clear_and_enable_dtpm_txt	Clears dTPM ownership and activates dTPM/TXT.
--clear_dtpm	Clears dTPM ownership and disables dTPM for TPM 1.2. Clears dTPM ownership for TPM 2.0.
--enable_txt_and_dtpm	Enables TXT and dTPM.
--clear_and_enable_dtpm	Clears dTPM ownership, disables dTPM (for TPM 1.2 only) and activates dTPM.
--disable_dtpm	Disables dTPM.
--disable_txt	Disables TXT.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c TpmManage [options…]
[--reboot]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmManage
--clear_and_enable_dtpm_txt --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmManage
--clear_dtpm --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmManage
--enable_txt_and_dtpm --reboot
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmManage
--clear_and_enable_dtpm --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmManage
--disable_dtpm --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmManage
--disable_txt --reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the TPM option is applied.

On platforms before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, use the command "TpmProvision" with options "--cleartpm and" --reboot to clear TPM module capabilities from managed systems. For detailed notes of the "—cleartpm" option usage, see *5.10.3 Providing and Clearing TPM Module Capabilities (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c TpmProvision  --
image_url <URL> [[--id <id for URL> --pw <password for URL>] | [--id <id for
URL> --pw_file <password file path>]] --cleartpm  --reboot
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmProvision  --image_url
'\\192.168.35.1\MySharedPoint\MyFolder' --id smbid --pw smbpasswd --cleartpm --
reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c TpmProvision  --image_url
'\\192.168.35.1\MySharedPoint\MyFolder' --id smbid --pw_file smbpasswd.txt --
cleartpm --reboot
```

```
SList.txt:
    192.168.34.56
    192.168.34.57

smbpasswd.txt:
smbpasswd
```

If the execution “Status” field for a managed system is SUCCESS, its TPM capabilities are cleared.

6.12 Policy-Based Update

Policy-Based Update (PBU) is used on updating BIOS for multiple managed systems. To run PBU, you need to create a policy file in XML format so that a policy action is applied to each system. The policy actions include "Update", "Reupdate", "OneFile" and "Ignore".

Currently PBU supports the command UpdateBios.

6.12.1 Updating the Managed System

Use the command "UpdateBios" with the BIOS firmware image SMCI_BIOS.rom to update the managed systems. For detailed usage notes of the "UpdateBios" command, see the usage notes in *5.3.2 Updating the BIOS Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateBios --policy
<policy XML file> [--precheck] [options…]
```

Option Commands	Descriptions
--reboot	Forces the managed systems to reboot.
--flash_smbios	Overwrites SMBIOS data.
--preserve_mer	Preserves ME firmware region.
--preserve_nv	Preserves NVRAM.
--preserve_setting	Preserves setting configurations.
--precheck	Used with the option --policy. The policy actions are not applied on corresponding managed systems; this option only shows the parsing result, without execution.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBios --policy
policy_sample.xml --precheck
```

```
SList.txt:
    192.168.34.56
    192.168.34.57

policy_sample.xml:

    Refer to next section for an example of XML file.
```

The execution progress for the managed system will be continuously updated to the "Execution Message" section in the log.

6.12.2 Format of Policy File

The policy file is in XML format. The XML root is **FirmwareUpdatePolicy** element. **FirmwareUpdatePolicy** element contains one **GeneralPolicy** element**,** one **GroupPolicy** element and one **IndividualPolicy** element**.**

In **GroupPolicy** element, it contains 0 or more **Group** elements. In **IndividualPolicy** element, it contains 0 or more **IndividualPolicy** elements.

```
<FirmwareUpdatePolicy>
    <GeneralPolicy>
        …
    </GeneralPolicy>
    <GroupPolicy>
        <Group ID="1">
            …
        </Group>
        …
    </GroupPolicy>
    <IndividualPolicy>
        <Individual ID="1">
            …
        </Individual>
        …
```

```
    </IndividualPolicy>
</FirmwareUpdatePolicy>
```

All GeneralPolicy element, Group element and IndividualPolicy element contain one BIOS element. The BIOS element defines the policy action for this policy. For details of a policy action, refer to section *6.12.4 Policy Actions (Single System)*.

```
<GeneralPolicy>
    <BIOS Policy="Ignore">
        <Folder> Change this to a valid BIOS folder path. </Folder>
        <File> Change this to a valid BIOS file path. </File>
    </BIOS>
</GeneralPolicy>
```

Group element and Individual element contain their own key elements used as matching rule. Any system matches the rule will be appliced to the corresponding policy action defined in BIOS element. For details of the matching rule, refer to section *6.12.3 Matching Rules*.

```
<Group ID="1">
    <GroupKey>
        <BoardID>Valid Board ID</BoardID>
        <CustomerID></CustomerID>
        <BoardProduct></BoardProduct>
        <SystemProduct></SystemProduct>
    </GroupKey>
    <BIOS Policy="Ignore">
        …
    </BIOS>
<Group ID="2">
<Individual ID="2">
    <IndividualKey>
        <Address>255.255.255.255</Address>
    </IndividualKey>
    <BIOS Policy="Ignore">
```

```
        …
    </BIOS>
</Individual>
```

Following is a complete example. Users have to modify some text to provide correct folder paths as file paths.

```
<?xml version="1.0"?>
<FirmwareUpdatePolicy>
    <GeneralPolicy>
        <BIOS Policy="Update">
        <!-- Define general policy for UpdateBIOS command -->
        <!-- Firmware matching: match by BoardID and CustomerID -->
        <!-- Supported Policies: Ignore/Update/Reupdate/OneFile -->
        <!--     Ignore      : Do not update -->
        <!--     Update      : Update to the latest in Folder -->
        <!--     Reupdate    : Update to the same BIOS -->
        <!--     OneFile     : Update to one specified BIOS file -->
            <Folder> Change this to a valid BIOS folder path. </Folder>
            <!-- For "Update/Reupdate" Policy -->
            <File> Change this to a valid BIOS file path. </File>
            <!-- For "OneFile" Policy -->
        </BIOS>
    </GeneralPolicy>

    <GroupPolicy>
        <Group ID="1">
            <GroupKey>
            <!-- Group keys to define a group -->
            <!-- Supported key: BoardID/CustomerID/BoardProduct/SystemProduct --
>
            <!-- Empty value: Skip the key if no value is assigned. -->
```

```
            <!-- Key combine: Use AND operator to combine multiple keys. -->
                <BoardID>Valid Board ID</BoardID>
                <!-- BoardID from GetBiosInfo command -->
                <CustomerID></CustomerID>
                <!-- OEM customer ID in DMI type 11 for OEM BIOS -->
                <BoardProduct></BoardProduct>
                <!-- Base board product name in DMI type 2 -->
                <SystemProduct></SystemProduct>
                <!-- System product name in DMI type 1 -->
                <Unique Designation=""></Unique>
                <!—- Data in Unique Firmware File Name -->
                <!—- Unique: string between first underline and second underline
of UFFN. -->
                <!—- Designation: STD/OEM, empty for not care -->
                <!-- E.g. BIOS_X12ABC-1234_20210101_2.0_STDsp -->
            </GroupKey>
            <BIOS Policy="Ignore">
                <Folder> Change this to a valid BIOS folder path. </Folder>
                <File> Change this to a valid BIOS file path. </File>
            </BIOS>
        </Group>
        <Group ID="2">
            <GroupKey>
                <BoardID>Valid Board ID</BoardID>
                <CustomerID></CustomerID>
                <BoardProduct></BoardProduct>
                <SystemProduct></SystemProduct>
                <Unique Designation=""></Unique>
            </GroupKey>
            <BIOS Policy="Ignore">
                <Folder> Change this to a valid BIOS folder path. </Folder>
```

```
                <File> Change this to a valid BIOS file path. </File>
            </BIOS>
        </Group>
    </GroupPolicy>

    <IndividualPolicy>
        <Individual ID="1">
            <IndividualKey>
            <!-- Individual keys to define an individual -->
            <!-- Supported key: Address -->
                <Address>255.255.255.255</Address>
                <!-- Network address for the managed BMC. -->
            </IndividualKey>
            <BIOS Policy="Ignore">
                <Folder> Change this to a valid BIOS folder path. </Folder>
                <File> Change this to a valid BIOS file path. </File>
            </BIOS>
        </Individual>
        <Individual ID="2">
            <IndividualKey>
                <Address>255.255.255.255</Address>
            </IndividualKey>
            <BIOS Policy="Ignore">
                <Folder> Change this to a valid BIOS folder path. </Folder>
                <File> Change this to a valid BIOS file path. </File>
            </BIOS>
        </Individual>
    </IndividualPolicy>
</FirmwareUpdatePolicy>
```

6.12.3 Matching Rules

Each managed system should apply a policy action. The Individual elements, Group elements and GeneralPolicy all contain their own policy actions. This section describles how SUM chooses the appropriate policy action for a managed system.

When finding an appropriate policy action for a managed system, the Individual element has the highest priority, then the Group element and finally the General element.

- If the address of a managed system matches the address in IndividualKey element, then the manage system applies the policy action of the Individual element.
- If the data of a managed system matches the values in GroupKey element, then the manage system applies the policy action of the Group element. A value is not used for comparison if it is empty. When comparing with the element values, all elements use the exact matching rule, except for the Unique element, which applies a partial comparison with Unique Firmware File Name.
  E.g. In a system with Unquie Firmware File Name "BIOS_**H12DSU-1B54**_20210118_2.0_**STD**sp", the H12DSU-1B54 is compared with the value of Unique element, the STD is compared with the Designation attribute.
  If users want to update a system with UFFN "BIOS_**H12ABC-1234-Ver-A**_20210101_2.0_**STD**sp" , BIOS image, and UFFN "BIOS_**H12ABC-1234-Ver-B**_20210110_2.0_**STD**sp", but ignore BIOS image with UFFN "BIOS_**H12ABC-1234-Special**_20210120_2.0_**STD**sp", they can set the Unique element with the **H12ABC-1234-Ver** value.
  When users only update BIOS from STD to STD, they can set the Designation attribute to “STD,” and SUM will ignore any OEM image, and vice versa.
- If a managed system does not match any Individual element and Group element, then it applies the policy action of General element.

6.12.4 Policy Actions

There are four types of policy actions.

- **Ignore**: Any system matched the policy will be ignored in the updating process. No action is taken on the system.

- **Update**: Any system matched the policy will be updated with the newest matched BIOS image in the target folder. The target folder path is the text of Folder element.
- **Reupdate**: Any system matched the policy will be updated with the same build date BIOS image if the BIOS image is available in the target folder. The target folder path is the text of Folder element.
- **OneFile**: Any system matched the policy will be updated with the BIOS image specified in the File element.

The rule "Update" and "Reupdate" uses the value of Folder element. The rule “OneFile” uses the value of File element. Each BIOS element has its own Folder element and File element; you can store BIOS files in different folders.

Example

```
<BIOS Policy="Update">
    <Folder>/home/</Folder>
    <File>/home/</File>
</BIOS>
```

6.12.5 Cache Files

When running PBU, SUM generates a file named "**record.cache**" in the used folders listed in the policy file in XML format. The cache file stores parsing result of BIOS files in the folder. This cache file can reduce the parsing time required for next execution.

You can remove /add files to BIOS file folders; however, a cache file cannot be updated when an existing BIOS file is changed, or a file is replaced with a differentone. When this happens, SUM may get wrong BIOS information from the cache file, and BIOS file mis-matched in update stage.

To prevent this problem, you can remove the cahce file in the folder if necessary, and SUM will rebuild the cache again in the next run.

To remove all cache files in current folder and sub folders in Linux, you can run the following commands.

```
# find . -name "record.cache" -type f

# find . -name "record.cache" -type f -delete
```

Notes:

- Do not put the non BIOS image files of these sizes, including 16 Mbytes, 32 Mbytes and 64Mbytes in folders used in PBU.
- A failure to parse BIOS image files will be treated as an error. And SUM treats files with data size of 16 Mbytes, 32 Mbytes and 64 Mbytes as BIOS image files.

6.12.6 Error Warning

All occurred errors are listed in SUM. When a critical error occurs, its warning message immediately appears. Two examples below illustrate how errors are shown on screen.

Example 1: A Typo in an XML File

```
Supermicro Update Manager (for UEFI BIOS) 2.4.0 (2019/09/16) (x86_64)
Copyright(C) 2013-2019 Super Micro Computer, Inc. All rights reserved.


*********************************<<<<<ERROR>>>>>*********************************

ExitCode                = 31
Description             = File management error
Program Error Code      = 431.2
Error message:
        General policy value >> Uppdate << is not a valid policy
Instruction:
        Fix XML file format errors

*****************************************************************************************
```

Example 2: Multiple Errors

```
Supermicro Update Manager (for UEFI BIOS) 2.4.0 (2019/09/16) (x86_64)
Copyright(C) 2013-2019 Super Micro Computer, Inc. All rights reserved.
.................
*******************************<<< Error List >>>*******************************
10.136.160.4 has no matched file by General Policy.
10.136.160.34 does not match firmwware file /home/user/BIOS/X11DPU/X11DPU9.119 by Group Policy.
10.136.160.7 does not match firmwware file /home/user/BIOS/X10SRL8.606 by Individual Policy.
10.136.160.31 has no matched file by General Policy.
10.136.160.141 cannot be connected.
10.136.160.24 has 2 files matched in the folder by General Policy.
    /home/user/BIOS/X11DAi-N_T20190116.bin
    /home/user/BIOS/Test/X11DAi-N_T20190116.bin
10.136.160.14 has no matched file by Individual Policy.

*********************************<<<<<ERROR>>>>>*********************************

ExitCode                = 61
Description             = Utility internal error
Program Error Code      = 428.2
Error message:
        Please fix listed errors and try again

*****************************************************************************************
```

- 10.136.160.4: Marked as Update by General Policy, but no BIOS files matched.
- 10.136.160.34: Assigned a specific file by OneFile. But the file is not for this system.
- 10.136.160.7: Same as above except that the file was assigned by Individual Policy.

- 10.136.160.31: Marked as Update by General Policy, but no BIOS files matched.
- 10.136.160.141: System not available. The address is wrong or the system has connection problems.
- 10.136.160.24: Multiple files matched with a system. It is regarded as an error because SUM cannot decide the file to be used.
- 10.136.160.14: Marked as “Update” by Individual Policy, but no BIOS files matched.

6.13 GPU Management for Multiple Systems

6.13.1 Getting GPU Information

Use the command “GetGpuInfo” to get the current NVIDIA GPU information from the managed systems. The GPU information output will be the same as that in *5.11.1 Getting GPU Information (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetGpuInfo
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetGpuInfo

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the “Status” field of a managed system is SUCCESS, the PSU information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.14 CPLD Management for Multiple Systems

6.14.1 Getting CPLD Firmware Image Information (Multiple Systems)

Use the command “GetCpldInfo” to receive the CPLD firmware image information from the managed system as well as the input CPLD firmware image. For details, see *5.12.1 Getting CPLD Firmware Image Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetCpldInfo [--file
<filename>]
```

```
Example:

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetCpldInfo --file
CPLD.bin

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution ”Status” field for the managed system is SUCCESS, the BMC information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.14.2 Updating the CPLD Firmware Image (Multiple Systems)

Use the command “UpdateCpld” with the CPLD firmware image CPLD.bin to update the CPLD of managed systems. For details, see notes in *5.12.2 Updating the CPLD Firmware Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateCpld --file
<filename> --reboot
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateCpld --file
CPLD.bin

SList.txt:
    192.168.34.56
    192.168.34.57
```

The execution progress for the managed system will be continuously updated to the “Execution Message” section of the managed system in the created log file.

Appendix A. SUM Exit Codes

Exit Code Number	Description
0	Successful
Others	Failed
GROUP1 (1~30) Command line parsing check failed	
1	GetOpt unexpected option code
2	Unknown option
3	Missing argument
4	No host IP/user/password
5	Missing option
6	Unknown command
7	Option conflict
8	Can not open file
9	File already exists
10	Host is unknown
11	Invalid command line data
12	Function access denied
GROUP2 (31~59) Resource management error	
31	File management error
32	Thread management error
33	TCP connection error
34	UDP connection error
35	Program interrupted and terminated
36	Required device does not exist

37	Required device does not work
38	Function is not supported
39	FTP server reports error
40	Http connection error
GROUP3 (60~79) File parsing errors	
60	Invalid configuration file
61	Utility internal error
62	Invalid input file
63	Invalid firmware flash ROM
64	Invalid download file
65	Invalid internal file
GROUP4 (80~99) IPMI operation errors	
80	Node Product key is not activated
81	Internal communication error
82	Board information mismatch
83	Does not support OOB
84	Does not support get file
85	File is not available for download
86	Required tool does not exist
87	IPMI standard error
GROUP5 (100~119) In-band operation errors	
100	Cannot open driver
101	Driver input/output control failed
102	Driver report: ****execution of command failed****

103	BIOS does not support this in-band command
104	Driver report: ****file size out of range****
105	Cannot load driver
106	Driver is busy. Please try again later
107	ROM chip is occupied. Please try again later
108	Kernel module verification error
109	This operation is prohibited
GROUP6 (120~199) IPMI communication errors	
120	Invalid Redfish response
144	IPMI undefined error
145	IPMI connect failed
146	IPMI login failed
147	IPMI execution parameter validation failed
148	IPMI execution exception occurred
149	IPMI execution failed
150	IPMI execution exception on slave CMM or unavailable
151	IPMI execution exception on module not present
152	IPMI execution only for CMM connected
153	IPMI execution on non-supported device
154	IPMI execution only for BMC connected
155	IPMI delivered invalid data
180	IPMI command not found
181	IPMI command IP format error
182	IPMI command parameter length invalid

GROUP7 (200~) Special Group	
200	System call failed
249	Special action is required
250	Managed firmware error
251	Rooted exception
252	Nested exception
253	Known limitation
254	Manual steps are required

Notes:

- When using in-band commands with --reboot option through SSH connection to the managed OS, SSH connection would be closed by the managed OS when the system starts to reboot.
- Exit code 66-77 is replaced with exit code 60 62 64 65 in version 2.5.0.

Appendix B. Management Interface and License Requirements

[Group] Command	Management Interface Supported		Node Product Key Required on the Managed System (SFT-OOB-LIC, or SFT-DCMS-SINGLE)
	Out-Of-Band (Remote)	In-Band (Local)	
[System Checks]			
CheckOOBSupport	**Yes**	**Yes**	Not Required
CheckAssetInfo	**Yes**	No	Required
CheckSystemUtilization	**Yes**	No	Required
CheckSensorData	**Yes**	No	Not Required
ServiceCalls	**Yes**	**Yes**	**Both SFT-DCMS-SINGLE and SFT-DCMS-SVC-KEY are required.**
[Key Management]			
ActivateProductKey	**Yes**	**Yes**	Not Required
QueryProductKey	**Yes**	**Yes**	Not Required
[BIOS Management]			
UpdateBios (without --preserve_setting)	**Yes**	**Yes**	Required for remote usage on H12 non-RoT systems and platforms before H12/X12
UpdateBios (with --preserve_setting)	**Yes**	**Yes**	Required
GetBiosInfo	**Yes**	**Yes**	Not Required
GetDefaultBiosCfg	**Yes**	**Yes**	Required
GetCurrentBiosCfg	**Yes**	**Yes**	Required
ChangeBiosCfg	**Yes**	**Yes**	Required **SFT-DCMS-SINGLE for some configuration items**
LoadDefaultBiosCfg	**Yes**	**Yes**	Required
GetDmiInfo	**Yes**	**Yes**	Required
EditDmiInfo	**Yes**	**Yes**	Required
ChangeDmiInfo	**Yes**	**Yes**	Required
SetBiosAction	**Yes**	**Yes**	Required
SetBiosPassword	**Yes**	**Yes**	Required
EraseOAKey	**Yes**	**Yes**	Not Required
BiosRotManage	**Yes**	**Yes**	**SFT-DCMS-SINGLE is required for Recover action**
[BMC Management]			
UpdateBmc	**Yes**	**Yes**	Not Required

GetBmcInfo	**Yes**	**Yes**	Not Required
GetBmcCfg	**Yes**	**Yes**	Required
ChangeBmcCfg	**Yes**	**Yes**	Required
LoadDefaultBmcCfg	**Yes**	**Yes**	Not Required
SetBmcPassword	**Yes**	**Yes**	Not Required
GetLockdownMode	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
SetLockdownMode	**Yes**	No	**SFT-DCMS-SINGLE only**
GetKcsPriv	**Yes**	**Yes**	Required
SetKcsPriv	**Yes**	No	Required
BmcRotManage	**Yes**	**Yes**	**SFT-DCMS-SINGLE is required for Recover action**
TimedBmcReset	**Yes**	**Yes**	Not Required
[System Event Log]			
GetEventLog	**Yes**	**Yes**	Required
ClearEventLog	**Yes**	**Yes**	Required
GetMaintenEventLog	**Yes**	**Yes**	Not Required
GetHostDump	**Yes**	No	**SFT-DCMS-SINGLE only**
ClearMaintenEventLog	**Yes**	**Yes**	Not Required
[CMM Management]			
UpdateCmm	**Yes**	No	Not Required
GetCmmInfo	**Yes**	**Yes**	Not Required
GetCmmCfg	**Yes**	No	Not Required
ChangeCmmCfg	**Yes**	No	Not Required
LoadDefaultCmmCfg	**Yes**	No	Not Required
SetCmmPassword	**Yes**	No	Not Required
GetBbpInfo	**Yes**	No	Not Required
UpdateBbp	**Yes**	No	Not Required
GetBladePowerStatus	**Yes**	No	Not Required
SetBladePowerAction	**Yes**	No	Not Required
[Storage Management]			
GetRaidControllerInfo	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
UpdateRaidController	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
GetRaidCfg	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
ChangeRaidCfg	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
GetSataInfo	**Yes**	No	Required
GetNvmeInfo	**Yes**	No	Required
SecureEraseDisk	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
SecureEraseRaidHdd	**Yes**	No	**SFT-DCMS-SINGLE only**
GetPMemInfo	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
UpdatePMem	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
[Applications]			
MountIsoImage	**Yes**	**Yes**	Required

UnmountIsoImage	**Yes**	**Yes**	Required
MountFloppyImage	**Yes**	**Yes**	Required
UnmountFloppyImage	**Yes**	**Yes**	Required
GetUsbAccessMode	**No**	**Yes**	**SFT-DCMS-SINGLE only**
SetUsbAccessMode	**No**	**Yes**	**SFT-DCMS-SINGLE only**
RawCommand	**Yes**	**Yes**	Not Required
LocateServerUid	**Yes**	**Yes**	Not Required
SetHttpBoot	**Yes**	**Yes**	Required
[PSU Management]			
GetPsuInfo	**Yes**	**Yes**	Required
UpdatePsu	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
GetPowerStatus	**Yes**	**Yes**	Not Required
SetPowerAction	**Yes**	**Yes**	Not Required
[TPM Management]			
TpmProvision	**Yes**	**No**	Required
GetTpmInfo (SMCI OTA)	**Yes**	**Yes**	Required
GetTpmInfo (Intel OTA)	**Yes**	**Yes**	Required
TpmManage (SMCI OTA)	**Yes**	**Yes**	Required
TpmManage (Intel OTA)	**Yes**	**Yes**	Required
[GPU Management]			
GetGpuInfo	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
[CPLD Management]			
GetCpldInfo	**Yes**	**Yes**	Not Required
UpdateCpld	**Yes**	**Yes**	Not Required

Appendix C. Known Limitations

General limitations
● For the --reboot option in OOB usage, if the target OS does not support software shutdown, system will be forced to power off and on again. ● The --post_complete option is designed for the system to wait for the managed system POST to complete and requires both BMC and BIOS. However, when the managed system lacks support from BIOS, no futher actions from SUM will be carried out even after the managed system POST is complete. ● All In-band commands through KCS on Windows require SD5 to be removed.

BIOS Management
● OOB UpdateBios command is not supported on motherboards that implement client ME such as X11SAE-F, X11SAT-F, X11SSZ-(Q)F/LN4F, X11SRM-VF, X11SBA-(LN4)F, X11SPA and X11SRi-IF. In addition, it is not supported on C7-series platforms. ● X9DRL-iF/3F MB does not support OOB BIOS update and OOB/in-Band DMI information related commands. ● With the Server ME embedded on the Supermicro system, the execution of the in-band command "UpdateBios" might fail when the Client ME driver (MEIx64) is installed on Windows. ● ChangeBiosCfg command will show error messages if the current BIOS configuration is different from the generated BIOS XML configuration file. ● BIOS XML configuration REQUIRES a text editor supporting extended ASCII characters (ISO-8859-1 encoding). ● The SW-managed JPME2 feature to update FDT in ME region is NOT supported in the following MBs: X11DDW-L/N(T) Revision 1.10, X11DPH-T-P Revision 1.00, X11DPL-I-P Revision 1.01, X11DPU-X(LL) Revision 1.01. Note that the earlier revisions of those four MBs are not supported neither. ● A1SRi/A1SAi MB does not support OOB BIOS update. ● Prevent BIOS downgrade if the ME version of current BIOS is greater than 4.0.4.294 and the ME version of updating BIOS is smaller than or equal to 4.0.4.294. ● Cascade Lake CPU only supports BIOS update of ME version 4.1 or higher version. ● TUI does not support mouse operation. ● OOB BIOS update on B1SA4, B11SRE and B11SCG-ZTF requires AC cycle. ● In-band update BIOS through KCS does not support on AMI platform. ● The format mm/dd/yy or mm/dd/yyyy is required for build date in DMI information. ● System will be powered off during update BIOS process on X12/H12 and later RoT platforms. ● The erase OA key function is not supported on the platforms before X12/H12. ● Neither updating BIOS In-band from version 1.x to 2.x, nor downgrading BIOS from version 2.x to 1.x on H12 non-RoT platforms through SMI is supported.

BMC Management

- In-band UpdateBmc command does not support AMI BMC firmware image.
- In-band GetBmcCfg/ChangeBmcCfg commands in Windows does not support a hostname that exceeds 244 bytes.
- In-Band UpdateBmc command on FreeBSD OS will be slow caused by KCS driver of FreeBSD.
- LAN table in BMC configuration file is read-only for OOB usage if BMC does not support REDFISH.
- For in-band and OOB usages, the file formats for receiving BMC settings may be different. Be careful of not misusing them.

CMM Management (OOB Only)

- All commands of CMM Management are for OOB use only.

Applications

- MountFloppyImage and UnmountFloppyImage commands do not support the X9 platforms.
- When dynamically enabling a USB port by the SetUsbAccessMode command , USB 3.0 devices may need to be manually unplugged and plugged back in to be available.
- The function of mounting ISO through IPv6 is not available on H12 AST2500 non-RoT platforms and versions before X12/H12.

PSU Management

- The UpdatePsu command only supports PSU "PWS-2K04A-1R" and "PWS-2K20A-1R".
- The UpdatePsu command does not support multi-OOB usage.

TPM Management

- The TpmProvision command does not support TPM 2.0 on Grantley.
- The TpmProvision command does not support on the platforms after Purley.
- While executing UpdateBIOS/In-Band TpmManage commands, manual steps are required under some special cases. Instructions will be provided to continue these commands.

GPU Management

- The GetGpuInfo command only supports NVIDIA GPU.

Key Management

- When activating JSON format key in Windows, the JSON key string cannot contain any spaces.

System Check

- You cannot access any cache files on mounted file systems with the ServiceCalls command.

Appendix D. Third-Party Software

The following open source libraries are used in SUM package:

Program	Library	License
sum	simpleopt	MIT
sum	pugixml	MIT
sum	Libcurl	MIT
sum	openssl	OpenSSL
sum	CryptoPP	Boost 1.0
sum	EDK2 Compress/Decompress	BSD
sum	Jsoncpp	MIT
sum	libarchive	OpenSSL
phymem.sys/pmdll.dll	phymem	CPOL
sum	ncurses	MIT
sum	PDCurses	MIT
ExternalData/tui.fnt	Terminus Font	OFL 1.1
sum	csv2	MIT
sum	UEFITool	BSD 2-Clause
sum	Sqlite	public domain
sum	Sqlite_orm	BSD 3-Clause
sum	CxxUrl	MIT

Appendix E. How to Change BIOS Configurations in XML Files

Five major setting types are provided as files in XML format: Numeric, CheckBox, Option, Password and String. The “Information” included in every setting is read-only. Executing the command ChangeBiosCfg does not affect the “information” enclosure. “Help” and “WorkIf” are two common fields in the “Information” enclosure of all settings. “Help” describes the target setting and “WorkIf” specifies the setting dependency. If the expression does not match the set conditions, a warning message will appear and the related setting will not be changed.

E.1 Numeric

In Information, it contains the maximum value “MaxValue”/minimum value “MinValue”, default value, and the amount to increase or decrease the value when a user requests a value change (StepSize) each time. “numericValue” is the value that you want to apply to BIOS setting. “Help” contains the explanation to the setting.

1. Open the XML file in Notepad++ (Windows) or vim (Linux).
2. Find the setting “Correctable Error Threshold” in the XML file.

```
<Setting name="Correctable Error Threshold" numericValue="10" type="Numeric">
  <Information>
    <MaxValue>32767</MaxValue>
    <MinValue>0</MinValue>
    <StepSize>1</StepSize>
     <DefaultValue>10</DefaultValue>
    <Help><![CDATA[Correctable Error Threshold (1 - 32767) used for sparing, tagging, and leaky bucket]]></Help>
  </Information>
</Setting>
```

3. Change the “numericValue” value in “Correctable Error Threshold.” In this example, the value is changed from 10 to 20.

```
<Setting name="Correctable Error Threshold" numericValue="20" type="Numeric">
```

4. Save the XML file and then execute the command “ChangeBiosCfg.”

E.2 CheckBox

In CheckBox, the allowed input value in “checkedStatus” would be marked as “Checked” or “Unchecked.” “checkedStatus” is the value that you want to apply to BIOS setting. “Help” contains the explanation to the setting.

1. Open the XML file in Notepad++ (Windows) or vim (Linux).
2. Find the setting “Serial Port 1” in the XML file.

```
<Setting name="Serial Port 1" checkedStatus="Checked" type="CheckBox">
  <!--Checked/Unchecked-->
  <Information>
    <DefaultStatus>Checked</DefaultStatus>
    <Help><![CDATA[Enable or Disable Serial Port (COM)]]></Help>
    <WorkIf><![CDATA[]]></WorkIf>
  </Information>
</Setting>
```

3. Change the “checkedStatus” value in “Serial Port 1.” In this example, the value is changed from Checked to Unchecked.

```
<Setting name="Serial Port 1" checkedStatus="Unchecked" type="CheckBox">
```

4. Save the XML file and then execute the command “ChangeBiosCfg.”

E.3 Option

In Option, you may choose one option in “AvailableOptions.” “selectedOption” is the value that you want to apply to BIOS setting. “Help” contains the explanation to the setting. The following procedures demonstrate how to change a setting with WorkIf dependency.

1. Open the XML file in Notepad++ (Windows) or vim (Linux).
2. Find the setting “When Log is Full” in the XML file.

```
<Setting name="When Log is Full" selectedOption="Do Nothing" type="Option">
   <Information>
      <AvailableOptions>
         <Option value="0">Do Nothing</Option>
         <Option value="1">Erase Immediately</Option>
      </AvailableOptions>
      <DefaultOption>Do Nothing</DefaultOption>
      <Help><![CDATA[Choose options for reactions to a full SMBIOS Event Log.]]></Help>
   <WorkIf><![CDATA[ ( 0 != SMBIOS Event Log ) ]]></WorkIf>
   </Information>
</Setting>
```

3. Change “selectedOption” from “Do Nothing” to “Erase Immediately”. Notice that there is “WorkIf” dependency “(0 != SMBIOS Event Log)” indicating that this setting is valid and can be modified only when the expression is evaluated true. That is, it is required to check the current value of setting “SMBIOS Event Log” as shown below.

```
<Setting name="SMBIOS Event Log" selectedOption="Disabled" type="Option">
   <Information>
      <AvailableOptions>
         <Option value="0">Disabled</Option>
         <Option value="1">Enabled</Option>
      </AvailableOptions>
      <DefaultOption>Enabled</DefaultOption>
      <Help><![CDATA[Change this to enable or disable all features of SMBIOS Event Logging during boot.]]></Help>
   </Information>
</Setting>
```

4. In “SMBIOS Event Log”, the selectedOption is “Disabled” which corresponds to the value 0. In other words, it makes the expression “(0 != SMBIOS Event Log)” false. In order to make it true, the selectedOption should be modified to “Enabled” as shown below.

```
<Setting name="SMBIOS Event Log" selectedOption="Enabled" type="Option">
```

5. Save the XML file and then execute command “ChangeBiosCfg.” After reboot, the “When Log is Full” should be changed to “Erase Immediately.”

E.4 Password

In Password, “NewPassword” and “ConfirmNewPassword” have to be the same. The password length is limited, as MinSize represents the minimum length and MaxSize represents the maximum length. “HasPassword” indicates whether the password is set or not. “Help” contains the explanation to the setting.

1. Open the XML file in Notepad++ (Windows) or vim (Linux).
2. Find the setting “Administrator Password” in the XML file.
3. Change “NewPassword” and “ConfirmNewPassword” in “Administrator Password.”

```
<Setting name="Administrator Password" type="Password">ss
  <Information>
    <Help>Set Administrator Password</Help>
    <MinSize>3</MinSize>
    <MaxSize>20</MaxSize>
    <HasPassword>False</HasPassword>
  </Information>
  <NewPassword><![CDATA[]]></NewPassword>
  <ConfirmNewPassword><![CDATA[]]></ConfirmNewPassword>
</Setting>
```

4. Save the XML file and execute command “ChangeBiosCfg.”
5. After reboot, the password takes effect and “HasPassword” becomes “True”.

E.5 String

In String, you can fill a string with the minimum “MinSize” and maximum “MaxSize” length. The option “AllowingMultipleLine” indicates that you can input multiple lines in “StringValue.” The default string value is “DefaultString.” “StringValue” is the value that you want to apply to BIOS setting. “Help” contains the explanation to the setting.

1. Open the XML file in Notepad++ (Windows) or vim (Linux).
2. Find the setting “KMIP Server IP address” in the XML file.

```
<Setting name="KMIP Server IP address" type="String">
 <Information>
  <MinSize>0</MinSize>
  <MaxSize>15</MaxSize>
  <DefaultString></DefaultString>
  <Help><![CDATA[Enter IPv4 address in dotted-decimal notation Example: 192.168.10.12]]></Help>
  <AllowingMultipleLine>False</AllowingMultipleLine>
  <LicenseRequirement>SFT-DCMS-SINGLE</LicenseRequirement>
 </Information>
 <StringValue><![CDATA[255.255.255.255]]></StringValue>
</Setting>
```

3. Change the “StringValue” in “KMIP Server IP address.”

```
<StringValue><![CDATA[127.0.0.1]]></StringValue>
```

4. Save the XML file and then execute command “ChangeBiosCfg.”

E.5.1 File Upload

SUM is allowed to upload files to BIOS, such as a TLS Certificate. In this case, there will be a comment <!--file path to load file--> under <StringValue> to indicate that file path should be filled. When executing the command “ChangeBiosCfg”, SUM will load the file from system and upload it to BIOS. The following example is the setting of TLS upload:

E.5.1.1 TLS Certificate

```
<Setting name="Enroll HTTPS Boot TLS Certificate" type="String">
 <Information>
  <MinSize>0</MinSize>
  <MaxSize>255</MaxSize>
  <DefaultString></DefaultString>
  <Help><![CDATA[Enroll HTTPS Boot TLS Certificate with type .cer,.der,.crt,.pem]]></Help>
  <AllowingMultipleLine>False</AllowingMultipleLine>
  <LicenseRequirement>SFT-DCMS-SINGLE</LicenseRequirement>
 </Information>
 <StringValue><![CDATA[]]></StringValue>
 <!--file path to load file-->
</Setting>
```

E.6 License Requirement

From SUM 2.5.0, SUM supports license requirement annotation for HII BIOS configuration. When the current BIOS supports license requirement annotation, the field “LicenseRequirement” is existed under the BIOS setting as the following example. The BIOS setting will only take effect when the activated product key level is greater than or equal to the license requirement.

Currently, the known BIOS feature categories requiring SFT-DCMS-SINGLE license are listed below:

- Lockdown Mode
- Security Erase related configuration
- KMIP related configuration
- PMem related configuration
- HTTP BOOT TLS certificate related configuration

Example:

```
<Setting name="Lockdown Mode" selectedOption="Disabled" type="Option">
        <Information>
        <AvailableOptions>
        <Option value="0">Disabled</Option>
        <Option value="1">Enabled</Option>
        </AvailableOptions>
        <DefaultOption>Disabled</DefaultOption>
        <Help><![CDATA[Switch Lockdown Mode]]></Help>
        <LicenseRequirement>SFT-DCMS-SINGLE</LicenseRequirement>
        </Information>
</Setting>
```

The supportness and limitatations are summarized in the following table.

	SUM 2.6.0 and later	SUM 2.5.x	SUM 2.4.0 and before
Managed system With SFT-DCMS-SINGLE	Take effect	May not take effect without a warning message	Not take effect No warning message
Managed system Without SFT-DCMS-SINGLE	Not take effect Output SFT-DCMS-SINGLE license required message	Not take effect May not output SFT-DCMS-SINGLE license required message	Not take effect No warning message

For SUM 2.4.0 and before, none of license SFT-DCMS-SINGLE required BIOS settings can be changed through SUM. Due to known limitation in SUM 2.5.x, even license SFT-DCMS-SINGLE is activated, SFT-DCMS-SINGLE required BIOS settings may not be able to change through SUM. To fully support, please use SUM 2.6.0 (or later) and pair with the feature supported BIOS. You must ensure that the activated product key level is greater than or equal to the license requirement to change license required BIOS settings. You can query the existed product key by QueryProductKey command, see *5.1.2 Querying the Node Product Keys*. If the activated product key level is less than the license requirement, you can activate another product key by ActivateProductKey command, see *5.1.1 Activating a Single Managed System*.

Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files

F.1 Introduction

XMLStarlet is a set of command line utilities which can be used to transform, query, validate, and edit XML files. Two examples are in the following sections.

F.2 Getting/Setting an XML Value (XML Element)

```
<?xml version="1.0"?>
<BmcCfg>
  <!--Usage notes:-->
  <!--You can remove unnecessary elements so that-->
  <!--their values will not be changed after update-->
  <!--Please refer to SUM User's guide '4.3 Format of the BMC Configuration Text File' for more details.-->
  <StdCfg Action="Change">
    <!--Supported Action:None/Change-->
    <!--Standard BMC configuration tables-->
    <FRU Action="None">
    <!--Supported Action:None/Change-->
      <Configuration>
      <!--Configuration for FRU data-->
        <BoardMfgName>SUPERMICRO</BoardMfgName>
```

- To get a value (SUPERMICRO) from an element from an xpath(/BmcCfg/StdCfg/FRU/Configuration/BoardMfgName) and a filename(BMCCfg.xml), run the command

  [shell]# xmlstarlet select --template -v "/BmcCfg/StdCfg/FRU/Configuration/BoardMfgName" BMCCfg.xml

- To set a value (SUPERMICRO) to an element in xpath(/BmcCfg/StdCfg/FRU/Configuration/BoardMfgName) and filename(BMCCfg.xml), run the command

  [shell]# xmlstarlet edit --inplace --update "/BmcCfg/StdCfg/FRU/Configuration/BoardMfgName" --value SUPERMICRO BMCCfg.xml

F.3 Getting/Setting an XML Value (XML Attribute)

```
<?xml version="1.0"?>
<BmcCfg>
  <!--Usage notes:-->
  <!--You can remove unnecessary elements so that-->
  <!--their values will not be changed after update-->
  <!--Please refer to SUM User's guide '4.3 Format of the BMC Configuration Text File' for more details.-->
  <StdCfg Action="Change">
    <!--Supported Action:None/Change-->
    <!--Standard BMC configuration tables-->
    <FRU Action="None">
```

- To get the value (None) from an attribute

  in xpath(/BmcCfg/StdCfg/FRU/@Action) and filename(BMCCfg.xml),

  run the command

  [shell]# xmlstarlet sel -t -v /BmcCfg/StdCfg/FRU/@Action BMCCfg.xml

- To set the value (None) to an attribute

  in xpath(/BmcCfg/StdCfg/FRU/@Action) and filename(BMCCfg.xml),

  run the command

  [shell]# xmlstarlet ed -L -P -u /BmcCfg/StdCfg/FRU/@Action -v None BMCCfg.xml

Appendix G. Removing Unchanged BIOS Settings in an XML File

Not all BIOS settings are intended to be changed in each update. In SUM, the unchanged settings can be removed from a configuration file. Metadata tags such as **<Subtitle>**, **<Text>** and **<Information>** are not parsed in the "ChangeBiosCfg" command and can be removed as well. In the example below, the XML tags are kept to a minimum:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<BiosCfg>
   <Menu name="Advanced">
      <Menu name="Boot Feature">
         <Setting name="Quiet Boot" checkedStatus="Checked" type="CheckBox">
         </Setting>
         <Setting name="Option ROM Messages" selectedOption="Force BIOS" type="Option">
         </Setting>
      </Menu>
   </Menu>
   <Menu name="Event Logs">
      <Menu name="Change SMBIOS Event Log Settings">
         <Setting name="MECI" numericValue="1" type="Numeric">
         </Setting>
      </Menu>
   </Menu>
   <Menu name="Boot">
      <Setting name=" Add boot option" type="String">
         <StringValue><![CDATA[]]></StringValue>
      </Setting>
   </Menu>
   <Menu name="Security">
      <Setting name="Administrator Password" type="Password">
         <CurrentPassword><![CDATA[]]></CurrentPassword>
```

```
        <NewPassword><![CDATA[]]></NewPassword>
        <ConfirmNewPassword><![CDATA[]]></ConfirmNewPassword>
      </Setting>
   </Menu>
</BiosCfg>
```

The first line is an XML declaration header. SUM specifies the encoding method as ISO-8859-1. If the text editor fails to deploy the encoding method ISO-8859-1, extended ASCII characters in a configuration file may be lost after the file is saved.

<BiosCfg> in the second line is the BIOS configuration root. In other words, SUM only attempts to parse child tags enclosed in <BiosCfg>. Within <BiosCfg>, the direct child tag must be <Menu>.

The **<Menu>** hierarchy represents the menu path in the BIOS configuration. Every setting has a menu path and the <Menu> hierarchy structure should always match. For example, the menu path for the setting "Quiet Boot" is "Advanced"->"Boot Feature". If "Advanced" is removed, SUM will try to find the match for "Quiet Boot" in the menu path "Boot Feature". Since the menu item "Boot Feature" is not in the first level of menu hierarchy in BIOS configuration in the managed system, an exception will be thrown.

In addition, for <Menu>, the attributes **"name"** and **"order"** (if applicable) should not be changed or removed. If any changes are made, a setting in the menu path will fail to match and SUM will export error messages. Similarly, for **<Setting>**, the attributes **"name"**, **"order"** (if applicable) and **"type"** should not be changed or removed. SUM will fail to identify a setting if those are changed.

In contrast, for the settings Option, CheckBox and Numeric, you can change the current values in the attributes **"selectedOption"**, **"checkStatus"** and "**numericValue"**, respectively. For the String setting, you can change the current contents in the child tag **<StringValue>**. For the Password setting, you can change the current password in the child tags **<CurrentPassword>** (if applicable), **<NewPassword>** and **<ConfirmNewPassword>**.

Appendix H. How to Sign a Driver in Linux

This example uses Red Hat Enterprise Linux 7 as the OS to illustrate the steps to sign a driver in Linux.

1. Install the following dependency utilities.

Syntax:

```
[shell]# sudo yum install <utility_name>
```

<utility_name> are listed below:

- openSSL
- kernel-devel
- mokutil
- keyutils
- perl (For Kernel version prior to 4.3.3)

2. Check if the option Secure Boot is enabled.

Syntax:

```
[shell]# sudo mokutil --sb-state
```

Example:

```
[root@localhost Linux]# sudo mokutil --sb-state
SecureBoot enabled
```

3. Check the OS keyring. The example SUM output below is from a Linux system where UEFI Secure Boot is enabled.

Syntax:

```
[shell]# sudo keyctl list %:.system_keyring
```

Example:

```
[root@localhost Linux]# sudo keyctl list %:.system_keyring
8 keys in keyring:
496952272: --alswrv      0     0 asymmetric: CentOS Linux kpatch signing key: ea0413152cde1d98ebdca3fe6f0230904c9ef717
332909815: --alswrv      0     0 asymmetric: Red Hat Inc.: 1ff96dd8d1b2327228c04b03a772dbb2dbb79b1f
406705284: --alswrv      0     0 asymmetric: CentOS Secure Boot (key 1): f037c6eaec36d4057a526c0ec6d5a95b324ee129
287390309: --alswrv      0     0 asymmetric: Microsoft Windows Production PCA 2011: a92902398e16c49778cd90f99e4f9ae17c55af53
983629943: --alswrv      0     0 asymmetric: Microsoft Corporation UEFI CA 2011: 13adbf4309bd82709c8cd54f316ed522988a1bd4
 22744187: --alswrv      0     0 asymmetric: AddTrust External CA Root: adbd987a34b426f7fac42654ef03bde024cb541a
 46692380: --alswrv      0     0 asymmetric: CentOS Linux kernel signing key: b70dcf0df2d9b7f29159248249fd6fe87b781427
384900254: --alswrv      0     0 asymmetric: CentOS Linux Driver update signing key: 7f421ee0ab69461574bb358861dbe77762a4201b
```

4. Configure the key information and follow the example below to create your own configuration file.

Example:

```
[ req ]
default_bits = 4096
distinguished_name = req_distinguished_name
prompt = no
string_mask = utf8only
x509_extensions = myexts
[ req_distinguished_name ]
O = <Your key name>
emailAddress = <Your Email>
[ myexts ]
basicConstraints=critical,CA:FALSE
keyUsage=digitalSignature
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid
```

Note: To create a key pair, a configuration file is needed. You can copy and paste the example above to create and name a configuration file as "configuration_file.config". Then modify the following variables in the configuration file.

- <Your key name>: the key name
- <Your e-mail>: the e-mail address

5. Generate a public and private X.509 key pair.

Syntax:

```
[shell]# sudo openssl req -x509 -new -nodes -utf8 -sha256 -days <days> -batch \
-config configuration_file.config -outform DER -out <public_key.der> -keyout \
<private_key.priv>
```

Notes:

- **<days>:** Valid certification days, e.g., 36500.
- **<public_key.der>:** The generated public key file, e.g., public_driver_key.der
- **<private_key.priv>:** The generated private key file, e.g., private_driver_key.priv

Example:

```
[root@localhost Linux]# sudo openssl req -x509 -new -nodes -utf8 -sha256 -days 36500 -batch -config configuration_file.config -outform
DER -out public_key.der -keyout private_key.priv
Generating a 4096 bit RSA private key
.....................................................................++
.........++
writing new private key to 'private_key.priv'
-----
```

6. Add your public key to the MOK list by using Linux mokutil.

Syntax:

```
[shell]# sudo mokutil --import public_key.der
```

Notes:

- You will be asked to enter and confirm a password for this MOK enrollment request.
- **public_key.der:** the generated public key file.

Example:

```
[root@localhost Linux]# sudo mokutil --import public_key.der
input password:
input password again:
```

7. Reboot the system and enroll the key.

Note: The MOK management main screen will appear immediately after reboot and last for 10 seconds. Please press any key as soon as you are under MOK management. If you miss this step, you will need to repeat step 6.

8. Press any key to continue.

9. Select **Enroll MOK**.

10. Select **Continue** to enroll the key.

Note: You can view your enrolled key by selecting **View key 0**.

11. Select **Yes**.
12. Input the password you set.
13. Select Reboot to reboot.
14. You will finish the setup upon entering Linux OS. Next, proceed with the steps in *2.3.2 Signing a* Driver in Linux to sign your key.

Appendix I. BMC/CMM Password Rule

I.1 X11/H11 and earlier platforms including H12 non-RoT systems

Since SUM 2.4.0, new password rules have been applied to X11/H11 and earlier platforms, including H12 non-RoT systems. You must use the following rules to create a BMC password.

- The password cannot be the reverse of the username.
- The password length is limited to 8 to 19 characters.
- The password must include characters from at least three of the following categories:
  - Alpha a-z
  - Alpha A-Z
  - Numeric 0-9
  - Special characters

The following table lists all supported special characters.

<space>	`	!	@	#	$	%	^
&	*	(	)	-	_	=	+
[	{	]	}	\	|	;	:
‘	“	,	<	.	>	/	?

I.2 X12/H12 and later platforms except H12 non-RoT systems

Since SUM 2.6.0, new password rules have been applied to X12/H12 and later platforms except H12 non-RoT systems. You must use the following rules to create a BMC password.

- The password cannot be reverse of or the same as user name.
- The password length is limited to 8 to 19 characters.
- The password must include characters from at least three of the following categories:
  - Alpha a-z
  - Alpha A-Z
  - Numeric 0-9
  - Special characters

The following table lists all supported special characters.

~	`	!	@	#	$	%	^
&	*	(	)	-	_	=	+
[	{	]	}	\	|	;	,
<	.	>	/	?			

I.3 CMM

Since SUM 2.4.0, new password rules have been applied to CMM. You must follow these rules to create a CMM password.

- The password length is limited to 8 to 19 characters.
- All special characters are supported except for <space>

The table lists all supported special characters.

!	$	%	&	(	)	*	+
.	/	<	=	>	?	@	[
\	]	^	_	`	{	|	}
~	-	:	,	;	#		

Appendix J. System Lockdown Mode Table

[Group] Command	Authority for System Lockdown Mode
	Read only
[System Checks]	
CheckOOBSupport	**Yes**
CheckAssetInfo	**Yes**
CheckSystemUtilization	**Yes**
CheckSensorData	**Yes**
ServiceCalls	No
[Key Management]	
ActivateProductKey	No
QueryProductKey	**Yes**
[BIOS Management]	
UpdateBios (without --preserve_setting)	No
UpdateBios (with --preserve_setting)	No
GetBiosInfo	**Yes**
GetDefaultBiosCfg	**Yes**
GetCurrentBiosCfg	**Yes**
ChangeBiosCfg	No
LoadDefaultBiosCfg	No
GetDmiInfo	**Yes**
EditDmiInfo	**Yes**
ChangeDmiInfo	No
SetBiosAction	No
SetBiosPassword	No
EraseOAKey	No
BiosRotManage	No
TimedBmcReset	No
[BMC Management]	
UpdateBmc	No
GetBmcInfo	**Yes**
GetBmcCfg	**Yes**
ChangeBmcCfg	No
SetBmcPassword	No
GetKcsPriv	**Yes**
SetKcsPriv	No

GetLockdownMode	**Yes**
SetLockdownMode	**Yes**
LoadDefaultBmcCfg	No
BmcRotManage	**Yes**
[System Event Log]	
GetEventLog	**Yes**
ClearEventLog	No
GetMaintenEventLog	**Yes**
ClearMaintenEventLog	No
GetHostDump	No
[CMM Management]	
UpdateCmm	No
GetCmmInfo	**Yes**
GetCmmCfg	**Yes**
ChangeCmmCfg	No
SetCmmPassword	No
LoadDefaultCmmCfg	No
GetBbpInfo	**Yes**
UpdateBbp	No
GetBladePowerStatus	**Yes**
SetBladePowerAction	No
[Storage Management]	
GetRaidControllerInfo	**Yes**
UpdateRaidController	No
GetRaidCfg	**Yes**
ChangeRaidCfg	No
GetSataInfo	**Yes**
GetNvmeInfo	**Yes**
SecureEraseRaidHdd	No
SecureEraseDisk	No
GetPMemInfo	**Yes**
UpdatePMem	No
[Applications]	
MountIsoImage	No
UnmountIsoImage	No
MountFloppyImage	No
UnmountFloppyImage	No
RawCommand	**Yes**
GetUsbAccessMode	**Yes**
SetUsbAccessMode	No
LocateServerUid	**Yes**
SetHttpBoot	No

[PSU Management]	
GetPsuInfo	**Yes**
UpdatePsu	**No**
GetPowerStatus	**Yes**
SetPowerAction	**Yes**
[TPM Management]	
TpmProvision	**No**
GetTpmInfo (SMCI OTA)	**Yes**
GetTpmInfo (Intel OTA)	**Yes**
TpmManage (SMCI OTA)	**No**
TpmManage (Intel OTA)	**No**
[GPU Management]	
GetGpuInfo	**Yes**
[CPLD Management]	
GetCpldInfo	**Yes**
UpdateCpld	**No**

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc.
	980 Rock Ave.
	San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information)
	support@supermicro.com (Technical Support)
Website:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V.
	Het Sterrenbeeld 28, 5215 ML
	's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information)
	support@supermicro.nl (Technical Support)
	rma@supermicro.nl (Customer Support)
Website:	www.supermicro.nl

Asia-Pacific

Address:	Super Micro Computer, Inc.
	3F, No. 150, Jian 1st Rd.
	Zhonghe Dist., New Taipei City 235
	Taiwan (R.O.C.)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Website:	www.supermicro.com.tw