Supermicro Update Manager

(SUM)

User’s Guide

Revision 2.11.0

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 2.11.0

Release Date: May 11, 2023

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 the --me_type option for the UpdateBios in-band command. 4. Added support from the UpdateBios in-band command to X10 MBs.
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.

Date	Rev	Description
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 the --reboot option. 3. Revised CheckSystemUtilization output message for HDD/Network. 4. Revised the 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 to exit code when using in-band command with the --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 the --image_url option. 3. Added support for checking SFT-SUM and SFT-DCMS-SINGLE node product keys. 4. Added a notice to the UpdateBios in-band command: The command will disable some functions in OS, but they will be recovered after OS reboot. 5. Added a notice to 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.”

Date	Rev	Description
		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 the BMC management commands: GetBmcInfo, UpdateBmc, GetBmcCfg, and ChangeBmcCfg. 2. Added in-band support for the EventLog management commands: GetEventLog and ClearEventLog. 3. Added in-band support for the CheckOOBSupport command. 4. Removed requirement of actool. 5. Removed JAVA environment requirement for all commands, except the OOB UpdateBios and UpdateBmc commands. 6. Changed the ActivateProductKey command: supports 344 bytes node product key format. 7. Added the 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 platforms. 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 the --overwrite_cfg and --overwrite_sdr options to the UpdateBmc

Date	Rev	Description
		command. 7. The UpdateBios in-band command supported the MEDisabling feature which has similar procedure as original jumperless procedure that requires twice reboot. 8. Added support for MountIsoImage and TpmProvision commands from HTTP image servers. 9. Added exit code 38: Function is not supported. 10. Added Feature Toggled On information to the 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 a TAS requirement note.
August-03-2016	1.6a	1. Renamed the TPM ISO image file to 20151217. 2. Added troubleshooting to BMC FW web server being unreachable after BMC FW was updated. 3. Added the description of failure to install Client ME Windows driver on a 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 GetDefaultBiosCfg and GetCurrentBiosCfg commands and deprecated the old GetDefaultBiosCfgTextFile and GetCurrentBiosCfgTextFile commands. 4. Added OOB support for the CMM management commands: GetCmmInfo,

Date	Rev	Description
		UpdateCmm, GetCmmCfg, and ChangeCmmCfg. 5. Modified the UpdateBios in-band command 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 --lock option to the TpmProvision command. 5. Revised the --image_url command format 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 the 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 GetCurrentBiosCfg. 3. Renamed the command GetDefaultBiosCfgTextFile to GetDefaultBiosCfg.

Date	Rev	Description
		4. Modified the CheckAssetInfo command to support 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 --preserve_setting option to 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 --skip_unknown option to the UpdateBios command. 11. Added support for checking the 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 --skip_bbs option to the ChangeBiosCfg command. 2. The CMM related commands do not require any licenses.
August-17-2018	2.1	1. Added the GetPsuInfo and UpdatePsu commands to manage the PSU firmware image. 2. Added the Get TpmInfo and TpmManage commands 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 the limitation that the --overwrite_sdr and --overwrite_cfg options have to coexist for ATEN BMC FW. 8. Added the SetBiosPassword command. 9. Added exit code 13 - Invalid argument.

Date	Rev	Description
		10. Added the --rc_path option.
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 the 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 -f option to load file contents as a 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 with the GetBiosInfo command. 5. Added LAN configurations notes to BMC settings update. 6. Added the --pw_file option to the SetBiosPassword command. 7. Added the --file_only option to multiple commands. 8. Added exit code 249 - Special action is required.

Date	Rev	Description
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 --kcs option to the UpdateBios command. 5. Added the GetKcsPriv and SetKcsPriv commands. 6. Added Appendix I. BMC/CMM Password Rule. 7. Added the --policy and --precheck options. 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 GetLockdownMode and SetLockdownMode commands. 3. Added Appendix J. System Lockdown Mode Matrix. 4. Added the SecureEraseDisk command. 5. Added support for the in-band mode of mountisoimage and unmountisoimage commands. 6. Added the GetGpuInfo command. 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. Moved 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 --key_file option to the

Date	Rev	Description
		ActivateProductKey command. 14. Added the Redfish Host Interface usage to the UpdateBios, UpdateBmc, ActivateProductKey and QueryProductKey commands. 15. Added the MountFloppyImage and UnmountFloppyImage commands. 16. Added the SecureEraseRaidHdd command. 17. Added the --backup option. 18. Added the --forward option. 19. Added the information about the node product key format to the CheckOOBSupport command. 20. Added the GetMaintenEventLog command. 21. Added the BiosRotManage and BmcRotManage commands. 22. Added the LoadDefaultBmcCfg and LoadDefaultCmmCfg commands. 23. Added the information about system's support for RoT features to the CheckOOBSupport command. 24. Added more options in the .sumrc file 25. Changed the example of running the QueryProductKey command.
October-08-2020	2.5.1	1. Added the --overwrite_ssl option to the UpdateBMC command. 2. Added the "Not TCG/SAT3 Supported" new device type to the SecureEraseDisk command. 3. Updated the usage of TPM in the user's guide. 4. Removed the --reboot option from the BmcRotManage --action UpdateGolden command.
December-24-2020	2.6.0	1. Added the GetCpldInfo and UpdateCpld commands. 2. Added the LocateServerUid command. 3. Added the GetBbpInfo, UpdateBbp, and CmmPowerStatus commands. 4. Added the GetPMemInfo and UpdatePMem commands.

Date	Rev	Description
		5. Updated X12 BMC/CMM Password Rules in *Appendix I. BMC/CMM Password Rule*. 6. Added a notice to the GetBmcCfg and ChangeBmcCfg commands. 7. Added the command ServiceCalls. 8. Added new descriptions to *1.1 Features*. 9. Added the --overwrite_sdr and --overwrite_ssl options to the UpdateCMM command. 10. Added the GetHostDump command. 11. Added the ClearMaintenEventLog command. 12. Added the --post_complete option 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 --controller option to the GetRaidControllerInfo and UpdateRaidController commands. 15. Added the Redfish Host Interface usage to the GetRaidControllerInfo and UpdateRaidController commands. 16. Added support for Broadcom 3008 and Marvell SE9230 to the GetRaidControllerInfo command. 17. Added support for Marvell SE9230 to the UpdateRaidController command. 18. Added the GetBladePowerStatus and SetBladePowerAction commands. 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

Date	Rev	Description
		commands.
December-15-2021	2.8.0	1. Added the commands UpdateAocNIC and GetAocNICInfo. 2. Deprecated the --policy and --precheck for UpdateBios options. 3. Added the --download option to the GetCmmCfg command. 4. Added the --upload and --update options to the ChangCmmCfg command. 5. Added the GetSystemCfg and ChangeSystemCfg commands. 6. Added the ProfileManage command. 7. Added the introduction to the profile update feature. 8. Added the RedfishApi command.
March-30-2022	2.8.1	1. Added AuthNone authentication to the in-band use of Redfish Host Interface. 2. Added the RemoteExec command. 3. Added *Appendix K. Using SUM to Run 3rd -Party Tools*. 4. Added support for HTTPS image server to the MountIsoImage command.
July-8-2022	2.9.0	1. Added the UpdateGpu command. 2. Added the Attestation command. 3. Added the GetSwitchInfo, UpdateSwitch and RebootSwitch commands. 4. Added the SystemPFA and MemoryHealthCheck commands. 5. Added the GetAipCpldInfo and UpdateAipCpld commands. 6. Added the GetGpuInfo command to X12/H12 and later platforms. 7. Added the description and option usage to the KmsManage command for KMS OEM configurations.

Date	Rev	Description
December-8-2022	2.10.0	1. Added the --port option for all commands. 2. Removed the --policy and --precheck options from the UpdateBios command. 3. Added BIOS management commands: GetScpInfo and UpdateScp. 4. Supported the management commands for ARM64: GetBmcInfo, UpdateBmc, GetScpInfo, UpdateScp, GetBiosInfo and UpdateBios. 5. Added *Appendix L. Creating Firmware Updating Tar File for OpenBMC*. 6. Added the CpuOnDemand command. 7. Added the GetPsysStatus and SetPsysStatus commands. 8. Added the GetFruInfo and RestoreFruInfo commands. 9. Added the remote in-band and remote Redfish host interface usages to the BIOS/BMC management commands. 10. Added the GetBmcUserList and SetBmcUserList commands. 11. Added the ControlNVMe command. 12. Added TwinPro Management commands: GetTpCfg and ChangeTpCfg. 13. Updated the license requirement for the UpdateBios command --preserve_setting in *Appendix B.* 14. Supported the In-band usage of the GetNvmeInfo command.
May-11-2023	2.11.0	1. Added the MonitorCDUStatus command. 2. Added the GetMultinodeEcInfo and UpdateMultinodeEc commands. 3. Added the GetBackplaneCpldInfo and UpdateBackplaneCpld commands. 4. Added the PCIeSwitch Management commands: GetPCIeSwitchInfo and UpdatePCIeSwitch. 5. Added the GetfixedBootCfg and ChangefixedBootCfg command. 6. Added the BootstrappingAccount command.

Date	Rev	Description
		7. Added the --showall option to the CheckSensorData command. 8. Added the ChangeFruInfo command. 9. Added the --showall option to the GetFruInfo command. 10. Added the --dump option to the GetBmcCfg command. 11. Added the --restore option to the ChangeBmcCfg command. 12. Added the SecureBootManage command. 13. Added the GetVmInfo and VmManage commands. 14. Added the RmcpManage command. 15. Added the --showall option to the GetBmcInfo command. 16. Removed the GetPsysStatus and SetPsysStatus commands.

Contents

1 Overview

The Supermicro Update Manager (SUM) can be used to manage the BIOS, BMC/CMM and RAID, SCP firmware image update and configuration update 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
    - Retrieves the BIOS firmware information of the managed system
    - Updates the System Control Processor (SCP) firmware image
    - Retrieves the System Control Processor (SCP) firmware information 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
  - Supports the readable text files of VROC configuration in XML format
  - Updates VROC configuration.
- 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
  - Invokes Redfish API
- CPLD Management
  - Updates CPLD firmware images
- AIP Management
  - Only retrieves the AIP CPLD information remotely
  - Updates AIP CPLD firmware images

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 Linux: Red Hat Enterprise Linux Server 7.6 (aarch64) or later: CentOS 7.6 (aarch64) or later Linux: Oracle 8.5 (aarch64) or later Linux: Rocky Linux 8.5 (aarch64) or later Linux: Debian 11.1.0 (aarch64) or later Linux: Ubuntu Server 20.04.3 (aarch64) 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)

The network communication protocol and ports below 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 UpdateRaidController	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 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	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 R12 OpenBMC platform: 2.9.1-v27 or later
CMM Version	ATEN platform (SMT_MBIPMI): 2.45 or later
BIOS Version	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 Version 1.0d or later for Ampere® Altra®/Altra® Max processor family on R12 platforms

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)

OS	Supported OS List	Program/Script
		• 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/SCP/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	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 BIOS Version 1.0d or later for Ampere® Altra®/Altra® Max processor family on R12 platforms
Operating System	Linux: Red Hat Enterprise Linux Server 4 updates 3 (x86_64) or later Linux: CentOS 4.3 (x86_64) or later

Environment	Requirements
	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 Linux: Red Hat Enterprise Linux Server 7.6 (aarch64) or later Linux: CentOS 7.6 (aarch64) or later Linux: Oracle 8.5 (aarch64) or later Linux: Rocky Linux 8.5 (aarch64) or later Linux: Debian 11.1.0 (aarch64) or later Linux: Ubuntu Server 20.04.3 (aarch64) 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 a BMC firmware image and an IPMI driver installed. The BMC firmware image should meet the following requirements.

Firmware Image	Requirement
BMC Version	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

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

2.1.1 Linux, Windows, and FreeBSD

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 Getting 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 Getting Node Product Keys from Supermicro

To get 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":"11111111111111111111222222222222222333333333333333ab
abababababababababababbabcdcdcdcdcdcdccdcdcddcdefefefefefefefeefefefefghghghghghghghghghghgh"}
}
```

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	<InterfaceName> (case sensitive) Redfish_HI = Executes in-band commands using Redfish Host Interface. Remote_INB = Executes in-band commands on remote systems. Remote_RHI = Executes in-band commands using Redfish Host Interface on remote systems.
-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>

Options	Description or usage
--oi	<OS IP address>
--ou	<OS user ID>
--op	<OS user password>
--os_key	<OS private key>
--os_key_pw	<OS private key password>
--version	Shows version information.
--port	<BMC/CMM/Command port(s)> The format is "RMCP:623,HTTPS:443". Supports these ports: 1. RMCP (for BMC/CMM OOB usage) 2. HTTPS (for BMC/CMM Redfish usage) (Will overwrite the ports in the .sumrc file) Each command may support more optional port(s). Please read the help message of each command.
--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 the intermediate status of all managed systems. (For multiple systems, only OOB managed systems are shown.)
--remote_sum	<set remote SUM path> to be executed in the remote managed system.
--remote_sum_rc_path	<set remote .sumrc file path> to be applied to the remote managed system.

System Check	
Commands	**Long Options**
CheckOOBSupport	None
CheckAssetInfo **(OOB only)**	None
CheckSensorData **(OOB only)**	--showall **(Optional)** Shows more sensor data information.

System Check	
Commands	**Long Options**
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.
SystemPFA	**--action** 1 = GetCurrentStatus 2 = Enabled 3 = Disabled **-I Redfish_HI (Optional)** Uses Redfish Host Interface to monitor the system and set up the predictive failure analysis of the system. (Only in-band usage is supported.) **--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.
MemoryHealthCheck	**--action** 1 = GetCurrentStatus 2 = Persistent 3 = Enable 4 = Disable **-I Redfish_HI (Optional)** Uses Redfish Host Interface to check the memory health of the system. (Only in-band usage is supported.) **--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

System Check	
Commands	**Long Options**
	reboot.
CpuOnDemand	**--action** 1 = GetHwInfo 2 = GetOnDemandState 3 = SetLicenseActivateCode 4 = EnablePPIN **-v** Prints extra info of CAP and registers in action 2 = GetOnDemandState. **--cpu_id <CPU ID>** CPU ID to indicate CPU socket. **--hw_id <Hardware ID>** Hardware ID to indicate the PPIN of the CPU socket. **--hw_id_file <Hardware ID file>** Hardware ID file with the format of "BMC MAC;CPU ID;PPIN". **--lac_file <LAC+ map file>** License file with the format of "PPIN;LAC+(s)". **--cfg_file <SDSi-agent config file>** SDSi-agent config file, only useful in action 2 = GetOnDemandState and specifying -v. **--skip_gap <Skip gap(s)>** Skips the gap of LAC revision ID and continues provisioning. **--squash <Squash into one file>** Squashes the state reports into one file in the format of "PPIN;State Report." **--plain_text <Output state as plain text>** Displays demand state in plain text. **--file <file name>** Save to file in action 1 = GetHwInfo and action 2 = GetOnDemandState or provide license file in action 3 = SetLicenseActivateCode.

System Check	
Commands	**Long Options**
	-I Redfish_HI (Optional) Uses Redfish Host Interface to proceed with CpuOnDemand actions. (Only in-band usage is supported.) **--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.
ChassisIntrusion	**--action**1 = Status 2 = Clear **-I Redfish_HI (Optional)**Uses Redfish Host Interface to proceed with ChassisIntrusion actions. (Only in-band usage is supported.)
GetFruInfo	**--file <file name> (Optional)** Saves the dumped FRU data to a file. **--overwrite (Optional)** Overwrites the output file. **--showall (Optional)** Gets all FRU info from the managed system. **--file_only (Optional)** Works with the --file option, and only reads FRU information from the input dumped FRU file. **--dump (Optional)** Works with the --file option, and dumps FRU data. **--dev_id <Device ID>(Optional)** Gets more FRUs from CMM. FRU ID: [1-19] or "ALL" 1 = CMM Master 2 = CMM Middle Plane 3 = CMM Switch(A1) 4 = CMM Switch(A2) 5 = CMM Switch(B1) 6 = CMM Switch(B2) 7 = CMM PSU(A1) 8 = CMM PSU(A2) 9 = CMM PSU(A3)

System Check	
Commands	**Long Options**
	10 = CMM PSU(A4) 11 = CMM PSU(B1) 12 = CMM PSU(B2) 13 = CMM PSU(B3) 14 = CMM PSU(B4) 15 = CMM FAN(1) 16 = CMM FAN(2) 17 = CMM FAN(3) 18 = CMM FAN(4) 19 = CMM Slave
RestoreFruInfo	**--file <file name>** Reads the dumped FRU file. **--individually (Optional)** Restores each BMC with the corresponding FRU info file individually.

ChangeFruInfo	**--item <item name>**
	Changes the FRU field of the managed system.
	CT = Chassis Type
	CP = Chassis Part Number
	CS = Chassis Serial Number
	BDT = Board Mfg. Date/Time ("YYYY/MM/DD HH:MM")
	BM = Board Manufacturer
	BPN = Board Product Name
	BS = Board Serial Name
	BP = Board Part Number
	PM = Product Manufacturer
	PN = Product Name
	PPM = Product Part/Model Number
	PV = Product Version
	PS = Product Serial Number
	PAT = Asset Tag
	--value <assignment value>
	Changes the value of the given FRU field.

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. **--individually (Optional)** Updates each system's BIOS settings with the corresponding configuration file individually. **--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

BIOS Management	
Commands	**Long Options**
	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. (Support is available on platforms before X11 with OEM BMC request only and can be only used with in-band.) **--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. **--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.) **--staged <action> (Optional)** Sets action to: 1 = update: The update process will start at the next system boot. 2 = abort: Aborts the previously staged update task. 3 = getinfo: Check whether if there was any pending staged update task. **--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. **--individually (Optional)** Gets BIOS information from each system with the corresponding configuration file individually.

BIOS Management	
Commands	**Long Options**
	--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. **--extract_measurement (Optional)** Works with --file, extract BIOS image file measurement. **--showall(Optional)** Prints the last BMC reset time. **-I Redfish_HI (Optional)** Uses the Redfish Host Interface for in-band updates. (Only in-band usage is supported.)
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. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--overwrite (Optional)** **Overwrites the output file.**
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. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--overwrite (Optional)** Overwrites the output file. **--tui (Optional)** Edits BIOS configuration with text-based user interface.

BIOS Management	
Commands	**Long Options**
	--compact (Optional) Generates a compact version of the BIOS configuration containing only the settings that have been changed in the text-based user interface.
ChangeBiosCfg	**--file <file name>** Updates the BIOS with the given configuration file. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--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.
LoadDefaultBiosCfg	**--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--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.

BIOS Management	
Commands	**Long Options**
	--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.

BIOS Management	
Commands	**Long Options**
	--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 **(In-band only)**	**--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 4 = DownloadEvidence **--file <file name> (Optional)** Works with --action DownloadEvidence. Saves the BIOS evidence to a file. **--overwrite (Optional)** Works with --action DownloadEvidence. Overwrites the output file. **--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.
GetScpInfo	**-I Redfish_HI (Optional)** Uses the Redfish Host Interface for in-band updates. (Only in-band usage is supported.)

UpdateScp	**--file <file name>** Updates the SCP with the given SCP image file. **--reboot** Forces the managed system to reboot or power up after operation. **-I Redfish_HI (Optional)** Uses the Redfish Host Interface for in-band updates. (Only in-band usage is supported.)
SecureBootManage	**--action <action>** Sets action to: 1 = Status 2 = Enable 3 = Disable 4 = Showdatabases 5 = UploadCertificate 6 = ResetAllKeysToDefault 7 = DeleteAllKeys 8 = DeletePK **--file_type <file type> (Optional)** Selects the type of secure boot key. The format of <file type> is “PK”, “KEK”, “db”, “dbr”, “dbt” or “dbx” (case sensitive). **--file (Optional)** Uploads secure boot key in the format of PEM. **--individually (Optional)** Updates each system secure boot keys individually with the corresponding configuration file. **-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band secure boot manages. **--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.
GetFixedBootCfg	**--file <file name> (Optional)** Updates the fixed BIOS boot order with the given configuration file. **--redfish** Updates the fixed BIOS boot order with the pure Redfish solution. **--overwrite (Optional)** Overwrites the output file.
ChangeFixedBootCfg	**--file <file name>** Updates the BIOS fixed boot order with the given configuration file. **--redfish** Updates the BIOS fixed boot order with the pure Redfish solution. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each fixed BIOS boot configuration with the corresponding

	configuration file individually.

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.) **--individually (Optional)** Updates BMC settings of each system with the corresponding configuration file individually. **--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 the 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. **--individually (Optional)** Gets information of BMC on each system with the corresponding configuration file individually. **--file_only (Optional)** Works with --file, and only reads BMC information from the input image file. **--extract_measurement (Optional)** Works with --file, and extracts BMC image file measurement.

BMC Management	
Commands	**Long Options**
	-I Redfish_HI (Optional) Uses the Redfish Host Interface for in-band updates. (Only in-band usage is supported.)
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. **--dump (Optional)** Dumps the read-only BMC configuration file. **--overwrite (Optional)** Overwrites the output file.
ChangeBmcCfg	**--file <file name>** Updates the BMC with the given configuration file. **--restore (Optional)** Restores the BMC configuration with the corresponding read-only 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. **--skip_unknown (Optional)** Skips the unknown tables or settings in the BMC configuration file.
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>**

BMC Management	
Commands	**Long Options**
	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 the user configuration. **--preserve_user_cfg** Preserves the 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 4 = DownloadEvidence **--file <file name> (Optional)** Works with --action DownloadEvidence. Saves the BMC evidence to a file. **--overwrite (Optional)** Works with --action DownloadEvidence. Overwrites the output file.
TimedBmcReset	**--immediate <immediately>(Optional)** Reset the BMC immediately. **--delay <BMC reset delay time> (Optional)** Delay reset time.

BMC Management	
Commands	**Long Options**
	Note: Delay time must be set within 1 to 60 minutes.
Attestation	**--action <action>** Sets action to: Dump List Download Delete GetInfo Comapre **--file <file name> (Optional)** File name for the measurement file on managed system or local storage. **--ref <file name> (Optional)** Referenced measurement file name for the measurement comparison. **--overwrite (Optional)** Overwrites the output file when downloading measurement file from managed system. **--showall (Optional)** Prints all items from the input measurement files. **--item <item name> (Optional)** Prints specified item from the input measurement files. **--file_only (Optional)** Works with --file, only reads measurement information from the input measurement files. **--root_cert <file name> (Optional)** Compares root certificate in the measurement file with this root certificate file. **--extract_certs <file name> (Optional)** Extract device identity certificate chain from the measurement file and save it as PEM chain file. **--nonce <nonce> (Optional)** Specify nonce for action Dump.
GetBmcUserList	None
SetBmcUserList	**--action <action>** Sets action to: 1 = Add 2 = Del 3 = Level 4 = SetPwd

BMC Management	
Commands	**Long Options**
	--user_id <user ID (Optional) The BMC user ID. **--user_name (Optional)** The BMC user name. **--user_password <user password> (Optional)** The BMC user password. **--user_privilege <user privilege> (Optional)** For privilege level: Administrator: 4 Operator: 3 User: 2 Callback: 1 No Access: 15 No Access is not supported on platforms later than X11/H11 .
BootStrappingAccount	**-I Redfish_HI (Optional)** Uses Redfish Host Interface to get/delete a bootstrapping account. (Only in-band usage is supported.) **--action <action>** Sets action to: 1 = CreateAccount 2 = DeleteAccount 3 = CheckAccount **--user_name <user name> (Optional)** Deletes a bootstrapping account with a user name.
RmcpManage	**--action <action>** Sets RMCP status with: 1 = GetInfo 2 = Enable 3 = Disable **--port <port> (Optional)** Command optional port(s). The format of <port> is “RMCP:623” or “623”. RMCP is served as a RMCP server port.

System Event Log	
Commands	**Long Options**
GetEventLog	**--file <file name> (Optional)** Saves the event log to a file. Prints the event log onscreen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file. **--redfish (Optional)** Enables pure Redfish support. **--raw_data (Optional)** Prints the raw data of each event log. **--redfish (Optional)** Enables pure Redfish support. **--no_banner (Optional)** Hides the version and copyright banner. **-I Redfish_HI (Optional)** Uses the Redfish Host Interface for in-band updates.
ClearEventLog	**--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--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> (Optional)** Enters the start time YYYYMMDD. **--et <end time> (Optional)** 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.

System Event Log	
Commands	**Long Options**
	--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	**-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band get BMC configuration. (Only in-band usage is supported.) **--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. **--individually (Optional)** Updates CMM on each system with the corresponding configuration file individually. **--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)**

CMM Management (OOB Only)	
Commands	**Long Options**
	Reads the CMM information from an input CMM image file. **--individually (Optional)** Gets CMM information from each system with the corresponding configuration file individually. **--showall (Optional)** Prints the BIOS, BMC, and ARM SUM information of the managed Blade 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. **--download (Optional)** Downloads the current CMM configuration file accessible for profile update from CMM. **--profile_repo (Optional)** Downloads the existing CMM profile from CMM. **--overwrite (Optional)** Overwrites the output file.
ChangeCmmCfg	**--file <file name>** Updates the CMM with the given configuration file. **--upload (Optional)** Uploads the CMM configuration file to CMM for profile update. **--update <update rule> (Optional)** Updates the CMM configurations with the existing profile on CMM. Supported update rule: [Apply] **--individually (Optional)** Updates each CMM with the corresponding configuration file individually. **--precheck (Optional)** Checks the configurations before update. **--skip_unknown (Optional)** Skips the unknown tables or settings in the CMM configuration file. **--skip_precheck (Optional)** Uploads and overwrites the existing CMM profile.
SetCmmPassword	**--user_id < user ID>** Enters the CMM user ID.

CMM Management (OOB Only)	
Commands	**Long Options**
	--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.**
ProfileManage	**--action <action>** Supported actions: Get, Edit, and Delete. **--file <file name> (Optional)** Saves the profile list to a file. Prints the profile list on screen if the file-saving function is not available. **--file_id <file ID> (Optional)** Gets, edits, or deletes the profile on the CMM with the specific file ID. **--profile_name <profile name> (Optional)** Edits the profile name on the CMM with the specific file ID. **--profile_description <profile description> (Optional)** Edits the profile description of the CMM with the specific file ID. **--schedule_update_time <schedule update time> (Optional)** Edits the profile's scheduled time to update on the CMM with the specific file ID. Format: [YYYY-MM-DD_HH:MM] **--overwrite** Overwrites the output file. **--showall** Gets the information of the profile associated with blade systems with the specific profile IDs.

CMM Management (OOB Only)	
Commands	**Long Options**
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 5 = softshutdown 24 = accycle **--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**
RawCommand	**--raw <raw command>** Input hex-value commands
GetUsbAccessMode **(Inband Only)**	None
SetUsbAccessMode **(Inband Only)**	**--panel <front/rear>** The panel to be set. **--enable**

Applications	
Commands	**Long Options**
	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	**--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--file <file name>** Uploads the TLS certificate in the formats of .cer, .der, .crt, or .pem. **--boot_name <boot description>** Description for HTTP boot. **--boot_lan <boot lan port>** Enter the LAN port for HTTP boot. **--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.
KmsManage	**--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--server_ip <server IP address> (Optional)** Enters a KMS server IP address.

Applications	
Commands	**Long Options**
	--second_server_ip <second server IP address> (Optional) Enters a second KMS server IP address. **--port <port> (Optional)** Command optional port(s). The format of <port> is "TCP:5696" or "5696". TCP is served as a the KMS server port. **--time_out <time out> (Optional)** Enters a KMS server connecting time-out. **--time_zone <time zone> (Optional)** Enters a correct time zone GMT+. **--client_username <client username> (Optional)** Enters a client identity: UserName. **--client_password <client password> (Optional)** Enters a client identity: Password. **--ca_cert <CA certificate file name> (Optional)** Uploads a CA certificate from the file. **--client_cert <client certificate file name> (Optional)** Uploads a client certificate from the file. **--pvt_key <private key file name> (Optional)** Uploads a client private key from the file. **--pvt_key_pw <private key password> (Optional)** Enters client private key PEM. **--file <file name> (Optional)** When the --action GetInfo option is specified, saves the OEM configuration to a file. Otherwise, updates the OEM settings with the given configuration file. **--action <action> (Optional)** Sets a KMS manage action to: 1 = GetInfo 2 = Probe 3 = DeleteCA 4 = DeleteCert 5 = DeletePvtKey 6 = DeleteAll **--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.
GetSystemCfg	**--file <file name>**

Applications	
Commands	**Long Options**
	Saves the configuration to a file. **--current_password <current password>** Checks the current BIOS Administrator password. **--download** Downloads the current Blade system configuration file accessible for profile update from the CMM. **--file_id <file ID>** Downloads the existing Blade system profile from the CMM with the specific file ID. **--overwrite** Overwrites the output file. **--dev_id <Device ID>** Selects a blade index and a node ID. Blade index: [A1-A14] or [B1-B14] Node ID: [1-4] Format: [A1_1] **--cur_pw_file <Current password file>** The specified file path to read the BIOS Administrator password.
ChangeSystemCfg	**--file <file name>** Updates the managed system with the given configuration file. **--current_password <current password>** Checks the current BIOS Administrator password. **--upload** Uploads the Blade system configuration file to the CMM for profile update. **--file_id <file ID>** Uses the ProfileManage command to access the list of profile file IDs. **--update <update rule>** Updates the Blade system configurations with the existing system profile on the CMM. Supported update rules: [Apply] or [Deploy] **--skip_precheck (Optional)** Uploads and overwrites the existing CMM profile. **--reboot** Forces the managed system to reboot or power up after operation.

Applications	
Commands	**Long Options**
	--dev_id <Device ID> Assigns a blade index and a node ID. Blade index: [A1-A14] or [B1-B14] Node ID: [1-4] Format: [A1], [A1_1] or [ALL] for all blade nodes **--skip_unknown** Skips the unknown settings or menus in the system configuration file. **--skip_bbs** Skips the BBS-related menus in the BIOS configuration file. **--precheck** Checks the configuration before the update. **--post_complete** Waits for the managed system to POST complete after reboot. **--cur_pw_file <Current password file>** **The specified file path to read BIOS Administrator password.**
RedfishApi	**-v** Verbose output: prints the response header. **-I Redfish_HI (Optional)** Uses Redfish Host Interface to query the firmware information. (Only available for in-band usage.) **--file <file name>** Outputs the result to a file. **--overwrite** Overwrites the output file. **--individually** Reads the request body from the particular file. (Only available for OOB usage on multiple systems.) **--request <HTTP method>** HTTP method (GET, POST, or PATCH) **--data <Request body>** Request body. **--retry <Number>** Number of retry times. The default value is 3.

Applications	
Commands	**Long Options**
RemoteExec	**-I Remote_INB** Manages the remote Linux systems and executes commands with in-band usage. **--remote_cmd <Remote command>** Enters the commands to be executed on remote Linux systems. **--file <file name>** Secure copies (scp) the file to remote Linux systems.

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 image file. **--controller <Controller>** <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.

Storage Management	
Commands	**Long Options**
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	**--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--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

Storage Management	
Commands	**Long Options**
	--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. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--cur_pw_file <Current Password File> (Optional)** The specified file path to read the current password. **--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

Storage Management	
Commands	**Long Options**
	image file.
GetVROCCfg	**-I Redfish_HI (Optional)** **--file <file name> (Optional)** Saves the configuration to a file. Prints the VROC configuration on the screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
ChangeVROCCfg	**-I Redfish_HI (Optional)** **--file <file name>** Updates the VROC with the given configuration file. **--individually (Optional)** Updates each VROC key with the corresponding configuration file individually.
ControlNVMe	**--action <action>** Sets action to: 1 = Locate 2 = StopLocate 3 = Insert 4 = Remove **--dev_id** NVMe device controller ID. **--group_id** NVMe device group ID. **--slot** NVMe device slot number.

NIC Management	
Commands	**Long Options**
GetAocNICInfo	**-I Redfish_HI (Optional)** Uses the Redfish Host Interface to query the firmware information. (Only in-band usage is supported.) **--file <file name> (Optional)** Reads the AOC NIC firmware information from an input AOC_NIC image file. **--dev_id <DEVICE_ID> (Optional)** AOC NIC device ID list.

NIC Management	
Commands	**Long Options**
UpdateAocNIC	**--file <file name>** Updates the AOC NIC with the given AOC_NIC image file. **--reboot** Forces the managed system to reboot or power up after operation. **--dev_id <Device ID>** Devce ID of AOC NIC. **-I Redfish_HI (Optional)** Uses the Redfish Host Interface for in-band updates. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.

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.

	-I Redfish_HI (Optional) Uses the Redfish Host Interface for in-band updates.
UpdateGPU	**--file <file name>** Updates the CEC/FPGA with the given GPU CEC/FPGA firmware file. **--item <item name>** FW item type of GPU firmware: 0 = CEC 1 = FPGA **-I Redfish_HI (Optional)** Uses the Redfish Host Interface for in-band updates.
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.) **--individually (Optional)** Gets CPLD information from each system with the corresponding configuration file individually. **--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. **--extract_measurement (Optional)** Works with --file, extract CPLD image file measurement.
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. **--individually (Optional)** Updates each CPLD with the corresponding configuration file individually. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.

AIP Management	
Commands	**Long Options**
GetAipCpldInfo **(OOB only)**	None
UpdateAipCpld **(OOB only)**	**--file <file name>** Updates the CPLD of AIP with the given FW image file. **--individually (Optional)**

	Updates the CPLD of AIP with the given FW image file.

TwinPro Management	
Commands	**Long Options**
GetTpCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the TwinPro configuration on the screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
ChangeTpCfg	**--file <file name>** Updates the TwinPro configuration with the given configuration file. **--individually (Optional)** Updates each set of TwinPro configurations with the corresponding configuration file individually.

CDU Management	
Commands	**Long Options**
MonitorCDUStatus	**--file <file name> (Optional)** Saves the CDU Status to the file or monitors the host with the given JSON file listing device and sensor data records to be monitored. **--action** Sets CDU action with: 1 = GetStatus 2 = SetCfg **--overwrite (Optional)** Overwrites the output file.

Backplane Management	
Commands	**Long Options**
GetMultinodeEcInfo	**-I Redfish_HI (Optional)** Uses the Redfish Host Interface to query the firmware information. (Only in-band usage is supported.) **--file <file name> (Optional)** Reads the multi-node EC firmware information from an input multi-node EC image file. **--file_only (Optional)** Works with the --file option, and only reads multi-node EC information from the input image file.

UpdateMultinodeEc	**--file <file name>** Updates the multi-node EC with the given multi-node EC image file. **-I Redfish_HI (Optional)** Uses Redfish Host Interface for in-band update.
GetBackplaneCpldInfo	None
UpdateBackplaneCpld	**--manual_ejected** Confirmed all drives on backplane have been ejected manually. **--file <file name> (Optional)** Updates the Backplane CPLD with the given FW image file. **--index <number> (Optional)** Updates the specific backplane CPLD with the given index. **--update_list <item list> (Optional)** Updates multiple backplane CPLDs with one command, using a comma (",") to distinguish between items. Item list example: 1:CPLD.jed,2:CPLD.jed…

VM Management	
Commands	**Long Options**
MountIsoImage	**-I Redfish_HI (Optional)** Uses the Redfish Host Interface to mount an ISO image. (Only in-band usage is supported.) **--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 the password
UnmountIsoImage	**-I Redfish_HI (Optional)** Uses the Redfish Host Interface to unmount an ISO image. (Only in-band usage is supported.)
MountFloppyImage	**--file <file name>** Mounts the specified binary floppy file to the managed system.
UnmountFloppyImage	None

VM Management	
Commands	**Long Options**
GetVmInfo	**-I Redfish_HI** Uses the Redfish Host Interface to get virtual media information. (Only in-band usage is supported.) **--dev_id <Device ID> (Optional)** Uses the specified device ID to get virtual media information
VmManage	**-I Redfish_HI** Uses the Redfish Host Interface to manage virtual media. (Only in-band usage is supported.) **--port <port> (Optional)** Command optional port(s) The format is "VM:623" or "623." Command optional port(s) list: 1. VM (for virtual media port) **--image_url <URL> (Optional)** 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 the password. **--dev_id <Device ID> (Optional)** The specified device ID to manage virtual media device. **--verify_cert (Optional)** Verifies the SSL certificate. (Only HTTPS protocol is supported.) **--accept_self_signed (Optional)** Accepts the self-signed certificate. (Only HTTPS protocol is supported.)

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 "/var/log/supermicro/SUM" folder 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 the --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 multiple systems execution.	.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 of ServiceCalls.	.sumrc file only
https_port	[1]443	[5]Sets managed system https port.	.sumrc file only

certificate	None	[6]Sets certificate files to verify the customized and 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 formats.

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

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

# set thread count for multiple systems usage
# thread_count = 50

# set retry count for multiple systems 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 “*name*=*value*” 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 the --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 "SetBiosAction" command 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 the 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). 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 "//" (two slashes).
- 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
<?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 “BroadcomRAIDController” and “MarvellRAIDController.”
- “Information,” “BroadcomRAIDController” and “MarvellRAIDController” 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 “BroadcomRAIDController” 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 “MarvellRAIDController” 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>
  <BroadcomRAIDController Action="Change" DeviceID="0" DeviceName="AVAGO
3108 MegaRAID">
    <!--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>
  <MarvellRAIDController 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 TwinPro Configuration XML File Format

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

```
<?xml version="1.0"?>
<TwinProCfg>
  <TwinProInfo>
    <!--Twin Pro information, this region is read only.-->
    <Information>
      <!--Twin Pro information, this region is read only.-->
      <MicroCloudSystem>False</MicroCloudSystem>
      <ConfigId>2</ConfigId>
      <!--Config ID-->
      <NodeA>
        <Power>Active</Power>
        <!--Node power, string value-->
        <IP>172.31.54.15</IP>
        <!--Node IP, string value-->
        <IPv6></IPv6>
        <!--Node IPv6, string value, only for Micro Cloud system-->
        <Watts>262W</Watts>
        <!--Node watts, string value-->
        <Current>21.3A</Current>
        <!--Node Current, string value-->
        <CPU1Temp>33C</CPU1Temp>
        <!--Node CPU1 Temperature, string value-->
        <CPU2Temp>28C</CPU2Temp>
        <!--Node CPU2 Temperature, string value-->
        <SystemTemp>23C</SystemTemp>
        <!--Node system Temperature, string value-->
        <NodePN></NodePN>
        <!--Node PN, string value-->
        <NodeSN>HM227S012083</NodeSN>
        <!--Node SN, string value-->
      </NodeA>
      <NodeB>
        <Power>Active</Power>
        <!--Node power, string value-->
        <IP>172.31.36.228</IP>
        <!--Node IP, string value-->
        <IPv6></IPv6>
        <!--Node IPv6, string value, only for Micro Cloud system-->
        <Watts>294W</Watts>
        <!--Node watts, string value-->
        <Current>24.1A</Current>
        <!--Node Current, string value-->
        <CPU1Temp>31C</CPU1Temp>
        <!--Node CPU1 Temperature, string value-->
        <CPU2Temp>29C</CPU2Temp>
        <!--Node CPU2 Temperature, string value-->
        <SystemTemp>20C</SystemTemp>
        <!--Node system Temperature, string value-->
        <NodePN></NodePN>
        <!--Node PN, string value-->
        <NodeSN>HM227S012108</NodeSN>
        <!--Node SN, string value-->
      </NodeB>
    </Information>
  </TwinProInfo>
  <CurrentNodeInfo Action="Change" Node="A">
    <!--Supported Action:None/Change-->
    <!--NodeId is current node ID-->
    <Information>
      <BackPlaneRevision>1.00</BackPlaneRevision>
      <!--BPN Revision-->
      <MCUVersion>0.12</MCUVersion>
      <!--MCU Version-->
    </Information>
    <Configuration>
      <SystemName>SystemName</SystemName>
      <!--System name, string value; length limit = 20 characters-->
```

```
      <SystemPN>SystemPN</SystemPN>
      <!--System PN, string value; length limit = 24 characters-->
      <SystemSN>SystemSN</SystemSN>
      <!--System SN, string value; length limit = 24 characters-->
      <ChassisPN>ChassisPN</ChassisPN>
      <!--Chassis PN, string value; length limit = 24 characters-->
      <ChassisSN>ChassisSN</ChassisSN>
      <!--Chassis SN, string value; length limit = 24 characters-->
      <BackPlanePN>BackPlanePN</BackPlanePN>
      <!--BackPlane PN, string value; length limit = 24 characters-->
      <BackPlaneSN>BackPlaneSN</BackPlaneSN>
      <!--BackPlane SN, string value; length limit = 24 characters-->
      <NodePN>NodePN</NodePN>
      <!--Node PN, string value; length limit = 24 characters-->
      <NodeSN>NodeSN</NodeSN>
      <!--Node SN, string value; length limit = 24 characters-->
      <ChassisLocation>00 00 00 00 00</ChassisLocation>
      <!--Chassis Location, Hex value-->
      <!--5 bytes, use spaces to separate-->
      <BackPlaneLocation>N/A</BackPlaneLocation>
      <!--FatTwin only, Valid value: Right/Left-->
      <!--Locations other than Right/Left, please fill in Hex vale.-->
      <!--Will be skipped if value is N/A-->
    </Configuration>
  </CurrentNodeInfo>
</TwinProCfg>
```

- The XML version is shown in the first line.
- The root table name is “*TwinProCfg*.” Its name tag pair is *<TwinProCfg>* and *</TwinProCfg>*. All information belonging to the root table is enclosed between this name tag pair.
- There could be two direct children for the root table: “*TwinProInfo*” and “*CurrentNodeInfo*.”
- “*TwinProInfo*” and “*CurrentNodeInfo*” 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 to the following element or table name tag. Each comment is enclosed by "*<!--*" and "*-->*" tags. The supported usages of each element and table are shown in the 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 specific table attributes in case they are needed.

In this example, in the TwinProInfo table, we can see the system has two nodes and both nodes are Active. From the CurrentNodeInfo table, the current node being configured is NodeA.

Notes:

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

4.10 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. Users 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. Users 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.

4.10.1 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 --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	TE127inuxnux	
FreeBSD	TE127inuxnux	

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 is shown 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.

4.10.2 BIOS TUI Configuration

4.10.2.1 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.

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.

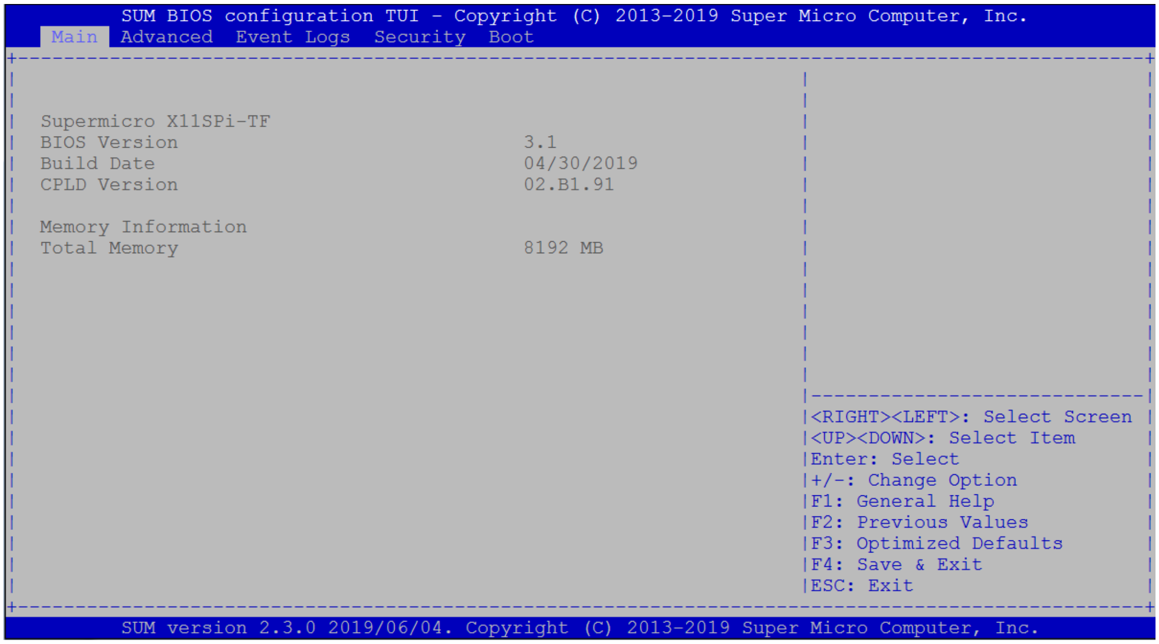
Notes:

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

4.10.2.2 How to Use

- **Using Arrow Keys**

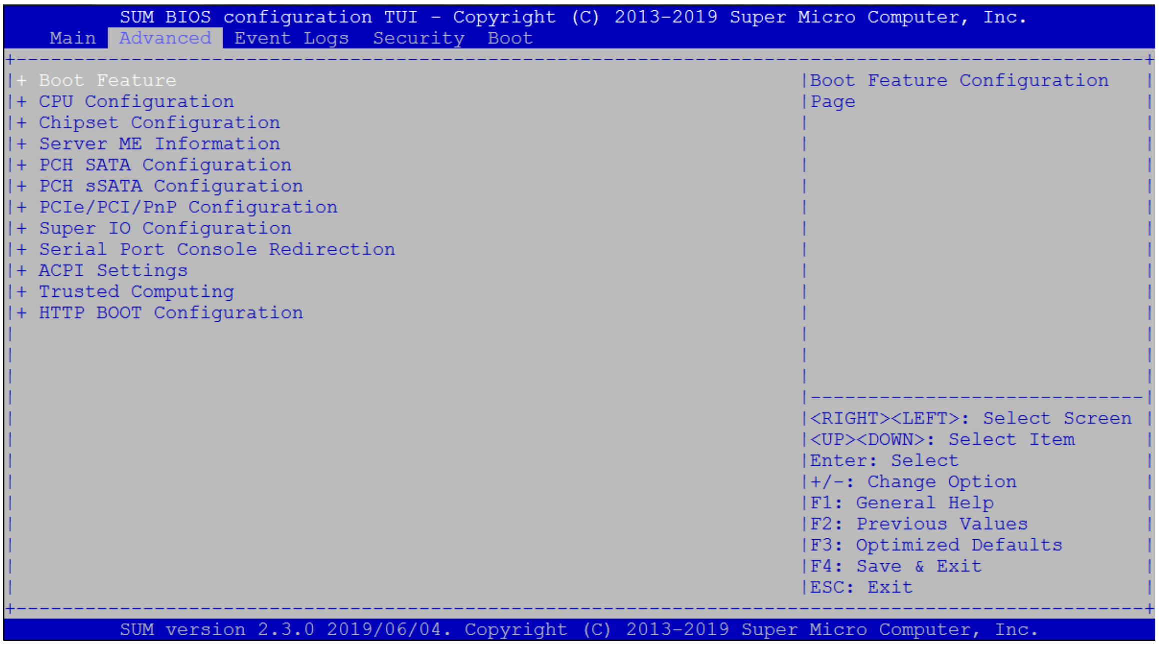
When you first enter the SUM BIOS Setup Utility, the “Main” root menu setup appears on screen. Press the arrow keys **<RIGHT>** and **<LEFT>** to navigate between menu tabs.



```
          SUM BIOS configuration TUI - Copyright (C) 2013-2019 Super Micro Computer, Inc.
   Main  Advanced  Event Logs  Security  Boot
+----------------------------------------------------------------------------------------------------+
|                                                                     |                              |
|                                                                     |                              |
|  Supermicro X11SPi-TF                                               |                              |
|  BIOS Version                              3.1                      |                              |
|  Build Date                                04/30/2019               |                              |
|  CPLD Version                              02.B1.91                 |                              |
|                                                                     |                              |
|  Memory Information                                                 |                              |
|  Total Memory                              8192 MB                  |                              |
|                                                                     |                              |
|                                                                     |                              |
|                                                                     |                              |
|                                                                     |                              |
|                                                                     |                              |
|                                                                     |                              |
|                                                                     |------------------------------|
|                                                                     |<RIGHT><LEFT>: Select Screen  |
|                                                                     |<UP><DOWN>: Select Item       |
|                                                                     |Enter: Select                 |
|                                                                     |+/-: Change Option            |
|                                                                     |F1: General Help              |
|                                                                     |F2: Previous Values           |
|                                                                     |F3: Optimized Defaults        |
|                                                                     |F4: Save & Exit               |
|                                                                     |ESC: Exit                     |
+----------------------------------------------------------------------------------------------------+
          SUM version 2.3.0 2019/06/04. Copyright (C) 2013-2019 Super Micro Computer, Inc.
```

- **Setting Values**

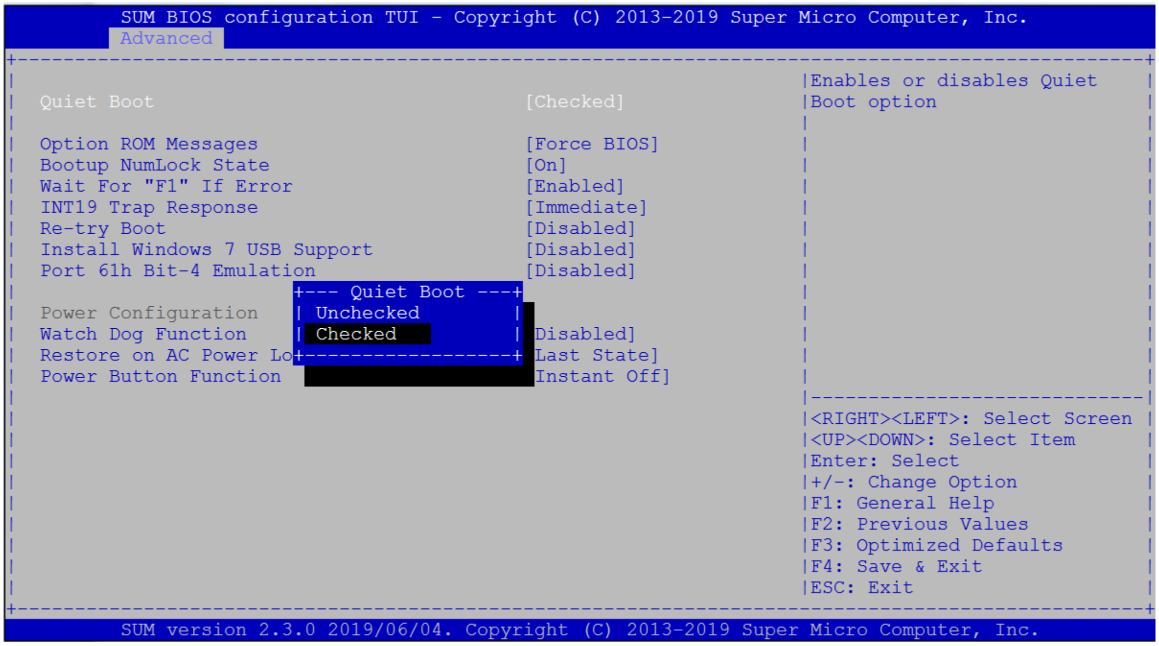
A “+” symbol before an option on a menu indicates that a sub-menu can be expanded for further configuration. To change a setting value, you can press the keys **<+>** and **<->**. Or you can press the **<Enter>** key to call up a dialog box for configuration.



```
          SUM BIOS configuration TUI - Copyright (C) 2013-2019 Super Micro Computer, Inc.
    Main  Advanced  Event Logs  Security  Boot
+----------------------------------------------------------------------------------------------------+
|+ Boot Feature                                                      |Boot Feature Configuration    |
|+ CPU Configuration                                                 |Page                          |
|+ Chipset Configuration                                             |                              |
|+ Server ME Information                                             |                              |
|+ PCH SATA Configuration                                            |                              |
|+ PCH sSATA Configuration                                           |                              |
|+ PCIe/PCI/PnP Configuration                                        |                              |
|+ Super IO Configuration                                            |                              |
|+ Serial Port Console Redirection                                   |                              |
|+ ACPI Settings                                                     |                              |
|+ Trusted Computing                                                 |                              |
|+ HTTP BOOT Configuration                                           |                              |
|                                                                    |                              |
|                                                                    |                              |
|                                                                    |                              |
|                                                                    |------------------------------|
|                                                                    |<RIGHT><LEFT>: Select Screen  |
|                                                                    |<UP><DOWN>: Select Item       |
|                                                                    |Enter: Select                 |
|                                                                    |+/-: Change Option            |
|                                                                    |F1: General Help              |
|                                                                    |F2: Previous Values           |
|                                                                    |F3: Optimized Defaults        |
|                                                                    |F4: Save & Exit               |
|                                                                    |ESC: Exit                     |
+----------------------------------------------------------------------------------------------------+
          SUM version 2.3.0 2019/06/04. Copyright (C) 2013-2019 Super Micro Computer, Inc.
```

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

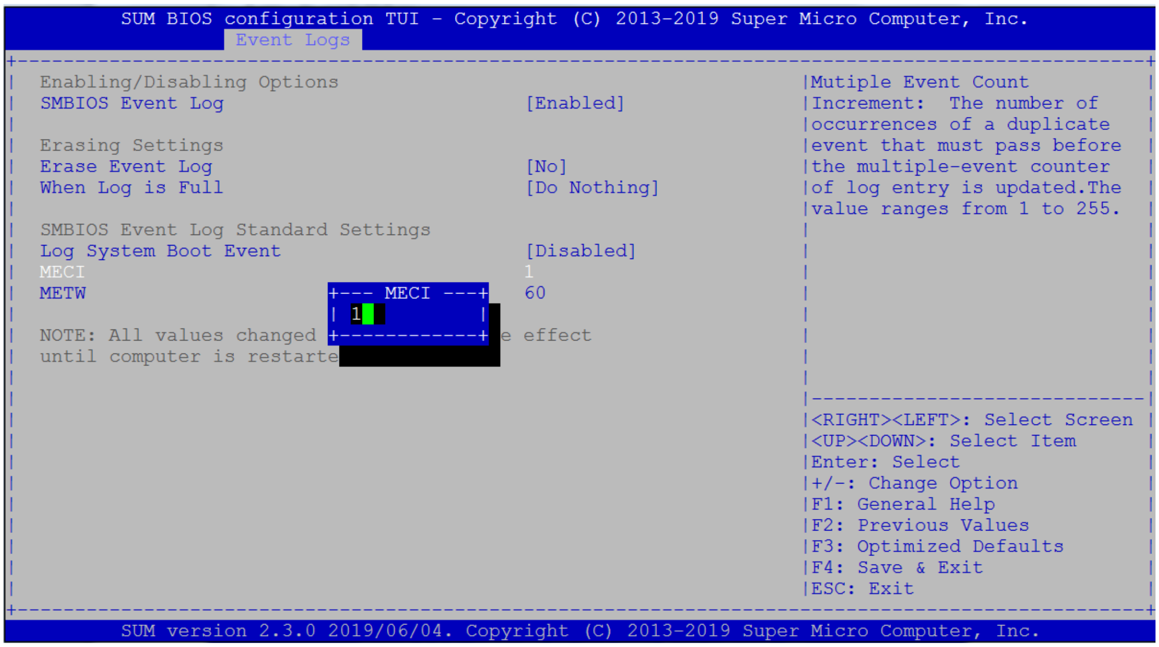
Some functions are allowed to be enabled or disabled. To change the setting, press the **<Enter>** key to call up a dialog box. Press the **<UP>** and **<DOWN>** arrow keys to make a selection. To disable a function, select **Unchecked**. To enable a function, select **Checked**.



```
          SUM BIOS configuration TUI - Copyright (C) 2013-2019 Super Micro Computer, Inc.
         Advanced
+-----------------------------------------------------------------------------------------+
|                                                            |Enables or disables Quiet   |
|  Quiet Boot                                [Checked]       |Boot option                 |
|                                                            |                            |
|  Option ROM Messages                       [Force BIOS]    |                            |
|  Bootup NumLock State                      [On]            |                            |
|  Wait For "F1" If Error                    [Enabled]       |                            |
|  INT19 Trap Response                       [Immediate]     |                            |
|  Re-try Boot                               [Disabled]      |                            |
|  Install Windows 7 USB Support             [Disabled]      |                            |
|  Port 61h Bit-4 Emulation                  [Disabled]      |                            |
|                        +--- Quiet Boot ---+                |                            |
|  Power Configuration   | Unchecked        |                |                            |
|  Watch Dog Function    | Checked          | Disabled]      |                            |
|  Restore on AC Power Lo+------------------+ Last State]    |                            |
|  Power Button Function                      Instant Off]   |                            |
|                                                            |----------------------------|
|                                                            |<RIGHT><LEFT>: Select Screen|
|                                                            |<UP><DOWN>: Select Item     |
|                                                            |Enter: Select               |
|                                                            |+/-: Change Option          |
|                                                            |F1: General Help            |
|                                                            |F2: Previous Values         |
|                                                            |F3: Optimized Defaults      |
|                                                            |F4: Save & Exit             |
|                                                            |ESC: Exit                   |
+-----------------------------------------------------------------------------------------+
          SUM version 2.3.0 2019/06/04. Copyright (C) 2013-2019 Super Micro Computer, Inc.
```

- **Setting Numeric Values**

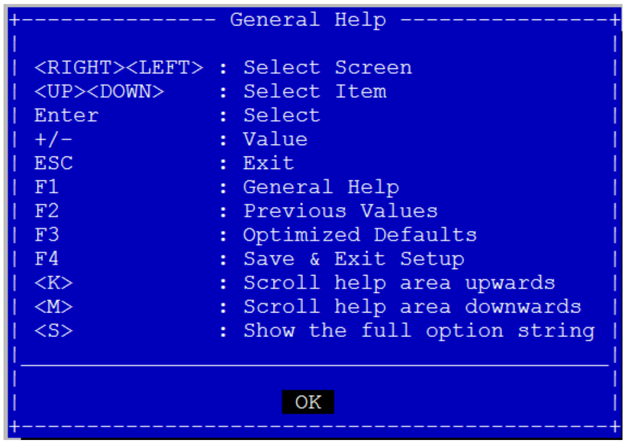
A value may be limited due to the BIOS. You can press the number keys to enter the desired value or press the **<+>** and **<->** keys to adjust your value within the range. If an input value is incorrect, a warning message appears on screen.



```
          SUM BIOS configuration TUI - Copyright (C) 2013-2019 Super Micro Computer, Inc.
                           Event Logs
+------------------------------------------------------------------------------------------------+
|  Enabling/Disabling Options                                           |Mutiple Event Count      |
|  SMBIOS Event Log                          [Enabled]                  |Increment:  The number of|
|                                                                       |occurrences of a duplicate|
|  Erasing Settings                                                     |event that must pass before|
|  Erase Event Log                           [No]                       |the multiple-event counter|
|  When Log is Full                          [Do Nothing]               |of log entry is updated.The|
|                                                                       |value ranges from 1 to 255.|
|  SMBIOS Event Log Standard Settings                                   |                          |
|  Log System Boot Event                     [Disabled]                 |                          |
|  MECI                                      1                          |                          |
|  METW                        +--- MECI ---+ 60                        |                          |
|                              | 1          |                           |                          |
|  NOTE: All values changed    +------------+ e effect                  |                          |
|  until computer is restarte                                           |                          |
|                                                                       |                          |
|                                                                       |--------------------------|
|                                                                       |<RIGHT><LEFT>: Select Screen|
|                                                                       |<UP><DOWN>: Select Item   |
|                                                                       |Enter: Select             |
|                                                                       |+/-: Change Option        |
|                                                                       |F1: General Help          |
|                                                                       |F2: Previous Values       |
|                                                                       |F3: Optimized Defaults    |
|                                                                       |F4: Save & Exit           |
|                                                                       |ESC: Exit                 |
+------------------------------------------------------------------------------------------------+
          SUM version 2.3.0 2019/06/04. Copyright (C) 2013-2019 Super Micro Computer, Inc.
```

4.10.2.3 Getting General Help

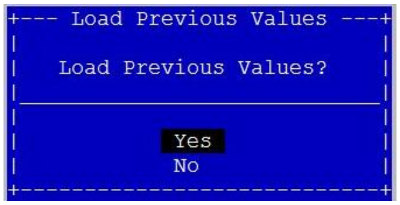
For general help information, press the **<F1>** key. A message box appears.



```
+--------------- General Help ----------------+
|                                              |
| <RIGHT><LEFT> : Select Screen                |
| <UP><DOWN>    : Select Item                  |
| Enter         : Select                       |
| +/-           : Value                        |
| ESC           : Exit                         |
| F1            : General Help                 |
| F2            : Previous Values              |
| F3            : Optimized Defaults           |
| F4            : Save & Exit Setup            |
| <K>           : Scroll help area upwards     |
| <M>           : Scroll help area downwards   |
| <S>           : Show the full option string  |
|                                              |
|                                              |
|                      OK                      |
+----------------------------------------------+
```

4.10.2.4 Loading Previous Values

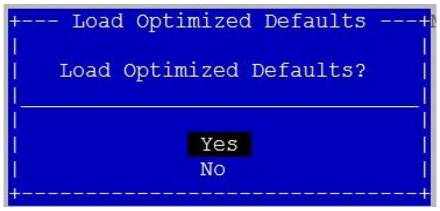
To load the previous values to all configurations, press the **<F2>** key. A message appears for confirmation.



```
+--- Load Previous Values ---+
|                            |
|   Load Previous Values?    |
|                            |
|                            |
|           Yes              |
|           No               |
+----------------------------+
```

4.10.2.5 Loading Optimized Values

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

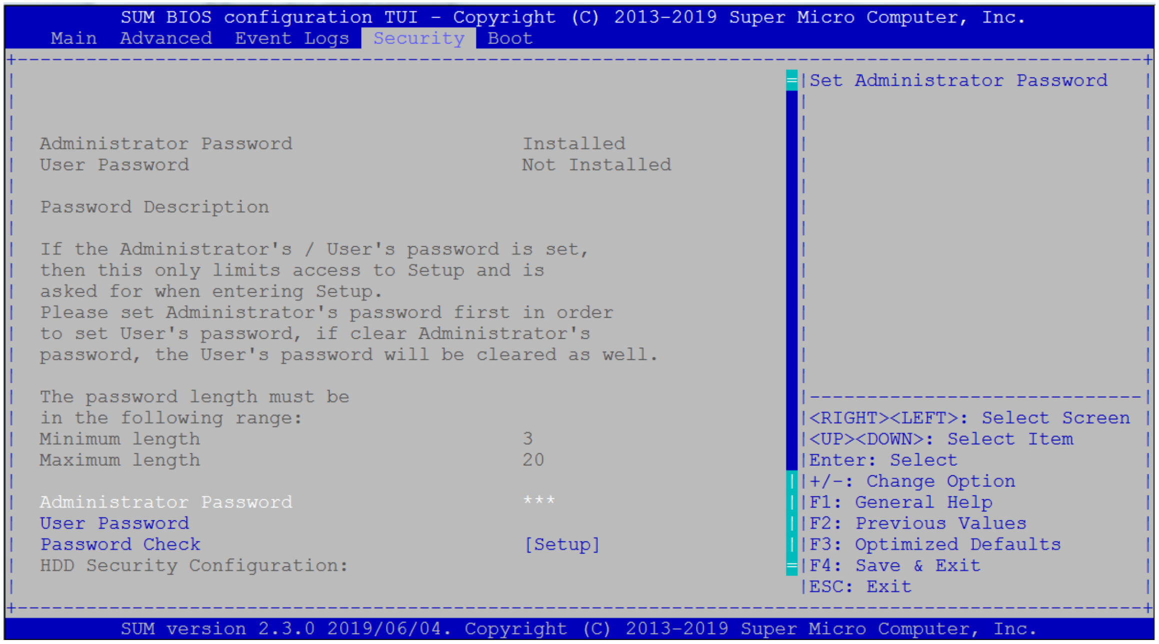


```
+--- Load Optimized Defaults ---+
|                               |
|   Load Optimized Defaults?    |
|                               |
|                               |
|            Yes                |
|            No                 |
+-------------------------------+
```

4.10.2.6 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:

- 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).

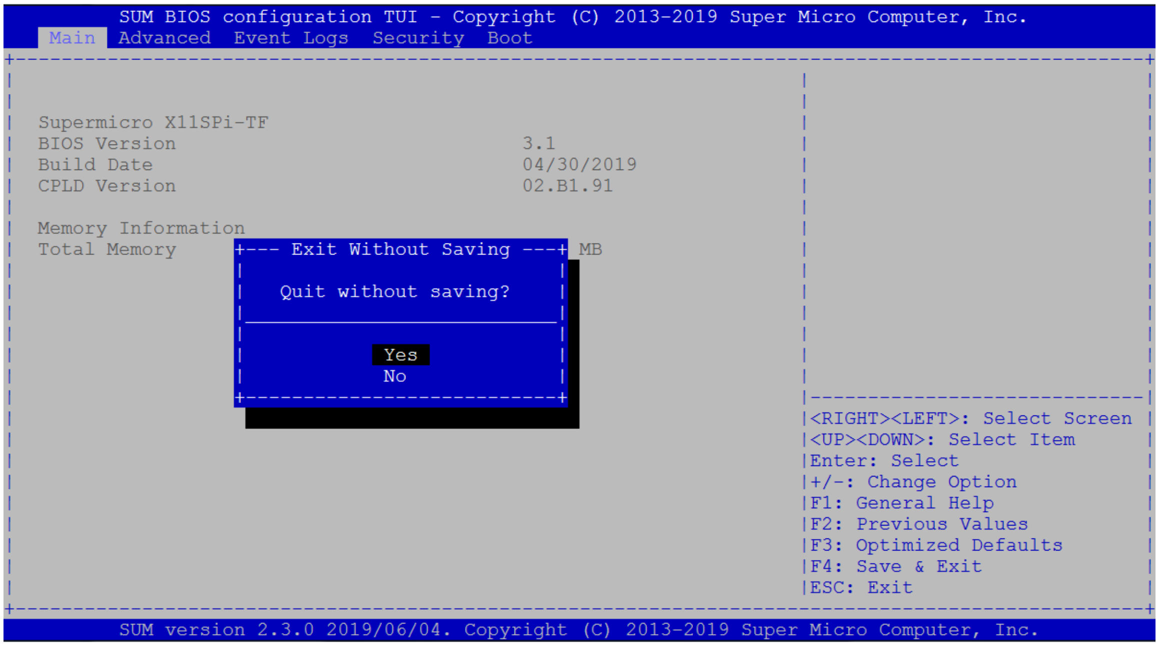


```
          SUM BIOS configuration TUI - Copyright (C) 2013-2019 Super Micro Computer, Inc.
    Main  Advanced  Event Logs  Security  Boot
+----------------------------------------------------------------------------------------------------+
|                                                                            |Set Administrator Password  |
|                                                                            |                            |
|                                                                            |                            |
|  Administrator Password                    Installed                       |                            |
|  User Password                             Not Installed                   |                            |
|                                                                            |                            |
|  Password Description                                                      |                            |
|                                                                            |                            |
|  If the Administrator's / User's password is set,                          |                            |
|  then this only limits access to Setup and is                              |                            |
|  asked for when entering Setup.                                            |                            |
|  Please set Administrator's password first in order                        |                            |
|  to set User's password, if clear Administrator's                          |                            |
|  password, the User's password will be cleared as well.                    |                            |
|                                                                            |                            |
|  The password length must be                                               |----------------------------|
|  in the following range:                                                   |<RIGHT><LEFT>: Select Screen |
|  Minimum length                            3                               |<UP><DOWN>: Select Item      |
|  Maximum length                            20                              |Enter: Select                |
|                                                                            |+/-: Change Option           |
|  Administrator Password                    ***                             |F1: General Help             |
|  User Password                                                             |F2: Previous Values          |
|  Password Check                            [Setup]                         |F3: Optimized Defaults       |
|  HDD Security Configuration:                                               |F4: Save & Exit              |
|                                                                            |ESC: Exit                    |
+----------------------------------------------------------------------------------------------------+
          SUM version 2.3.0 2019/06/04. Copyright (C) 2013-2019 Super Micro Computer, Inc.
```

4.10.2.7 Exiting the TUI

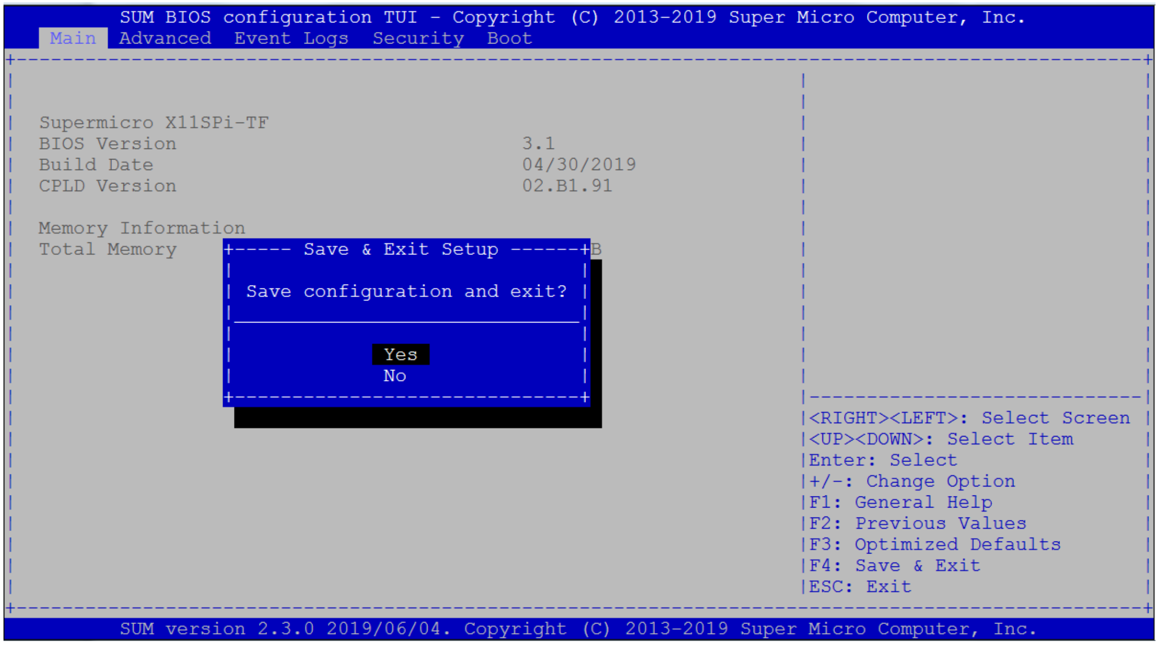
Two methods are available to exit the SUM BIOS configuration TUI.

- 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.



```
          SUM BIOS configuration TUI - Copyright (C) 2013-2019 Super Micro Computer, Inc.
   Main  Advanced  Event Logs  Security  Boot

  Supermicro X11SPi-TF
  BIOS Version                          3.1
  Build Date                            04/30/2019
  CPLD Version                          02.B1.91

  Memory Information
  Total Memory       +--- Exit Without Saving ---+ MB

                        Quit without saving?

                                 Yes
                                 No
                                                      |<RIGHT><LEFT>: Select Screen
                                                      |<UP><DOWN>: Select Item
                                                      |Enter: Select
                                                      |+/-: Change Option
                                                      |F1: General Help
                                                      |F2: Previous Values
                                                      |F3: Optimized Defaults
                                                      |F4: Save & Exit
                                                      |ESC: Exit
          SUM version 2.3.0 2019/06/04. Copyright (C) 2013-2019 Super Micro Computer, Inc.
```

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



```
          SUM BIOS configuration TUI - Copyright (C) 2013-2019 Super Micro Computer, Inc.
   Main  Advanced  Event Logs  Security  Boot
+----------------------------------------------------------------------------------------------------+
|                                                                    |                              |
|                                                                    |                              |
|  Supermicro X11SPi-TF                                              |                              |
|  BIOS Version                              3.1                     |                              |
|  Build Date                                04/30/2019              |                              |
|  CPLD Version                              02.B1.91                |                              |
|                                                                    |                              |
|  Memory Information                                                |                              |
|  Total Memory      +----- Save & Exit Setup ------+B               |                              |
|                    |                              |                |                              |
|                    | Save configuration and exit? |                |                              |
|                    |                              |                |                              |
|                    |                              |                |                              |
|                    |             Yes              |                |                              |
|                    |             No               |                |                              |
|                    +------------------------------+                |------------------------------|
|                                                                    |<RIGHT><LEFT>: Select Screen |
|                                                                    |<UP><DOWN>: Select Item      |
|                                                                    |Enter: Select                |
|                                                                    |+/-: Change Option           |
|                                                                    |F1: General Help             |
|                                                                    |F2: Previous Values          |
|                                                                    |F3: Optimized Defaults       |
|                                                                    |F4: Save & Exit              |
|                                                                    |ESC: Exit                    |
+----------------------------------------------------------------------------------------------------+
          SUM version 2.3.0 2019/06/04. Copyright (C) 2013-2019 Super Micro Computer, Inc.
```

4.11 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.

Notes:

- The Redfish Host Interface is not enabled by default in Linux. To enable the Redfish Host Interface in Linux, enable_RHI.sh in the SUM release package under the /script folder.
- For SUSE12 system, if the Redfish Host Interface is still not working after RHI.sh is enabled, you can execute SuSE12 _Firewall_WhiteList.sh in the SUM release package under /script/SUSE to add the Redfish Host Interface to the firewall whitelist.

4.11.1 Using Redfish Host Interface

Syntax:

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

Different from the standard in-band operation, you need <username> and <password> to access the managed system.

4.11.2 Supported Commands

Currently, the following commands support Redfish Host Interface for in-band usage: UpdateBios, UpdateBmc, ActivateProductKey, QueryProductKey, BiosRotManage, BmcRotManage, UpdateRaidController,GetRaidControllerInfo, UpdateAocNIC, GetAocNICInfo, GetCpldInfo, UpdateCpld, GetPMemInfo, UpdatePMem, GetBiosInfo, GetScpInfo, UpdateScp, GetBmcInfo, SecureBootManage, GetFixedBootCfg, ChangeFixedBootCfg, GetMultinodeEcInfo and UpdateMultinodeEc.

Example:

In-Band:

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

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

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetHostDump --action 1 -
-file log.tgz
```

4.11.3 AuthNone Authentication

Since SUM 2.8.1, SUM has supported AuthNone authentication for use on the in-band Redfish Host Interface. As a BMC OEM feature, AuthNone authentication requires the OEM BMC firmware to function properly. You can execute all SUM commands supporting -I Redfish_HI without a BMC username and a password.

Syntax:

```
sum -I Redfish_HI -c <command>
```

Example:

```
[SUM_HOME]# ./sum -I Redfish_HI -c BmcRotManage --action GetInfo
```

4.12 Format of the VROC Configuration XML File

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

- The XML version is shown in the first line.
- The root table name is "*VROCCfg*. " *<VROCCfg>* and *</VROCCfg>* are its tag pair. All information in the root table is enclosed between this tag pair.
- There could be two child tags for the root table: "*PhysicalDriveInfo*" and "*VolumeInfo*."
- The "PhysicalDriveInfo" and "VolumeInfo" root tables could have child tables.
- Configurable elements are listed in the "*Configuration*" fields in 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.
- To create a logical volume, the VolumeInfo action should be "*Change*" and the Volume action should be "*Create*." The "*PhysicalDriveList*" field must contain all VROC IDs or serial numbers for VROC creation and the "VROCId" field should be set to "-1."
- To delete a logical volume, the VolumeInfo action should be "*Change*," the Volume action should be "*Delete,*" and the corresponding VROC ID should be specified.
- To delete all arrays built in the VROC controller, the VolumeInfo action should be "*ClearAll*." If the action is "ClearAll," the VROC ID is irrelevant.
- To change the VROC configuration, you have to delete the original VROC controller and create a new VROC controller with the modified "*Name*," "*Level*," "*PhysicalDriveList*," "StripSize," and "Capacity" fields.

Notes:

- Child tables or configurable elements can be deleted to skip the updates for these tables or configuration elements.
- Child tables or configurable elements must stick to the parent tables.
- 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*.
- Supported RAID level is variant to VROC key on the motherboard. Supported RAID level:

Supermicro PN	Description	RAID Support
AOC-VROCINTMOD	Intel SSD Only Upgrade module	RAID 0/1/10/5
AOC-VROCSTNMOD	Standard Upgrade module	RAID 0/1/10
AOC-VROCPREMOD	Premium Upgrade module	RAID 0/1/10/5

- For Intel PCIe Gen3 x8 SSDs, an Intel VROC hardware key is not required to use RAID 0, while a hardware key is required to use RAID 0/1/5/10 for most SSDs.
- For details on VROC key, please refer to Supermicro website: https://www.supermicro.com/en/products/accessories/addon/AOC-VROCxxxMOD.php

Example:

```
<?xml version="1.0"?>
<VROCCfg>
  <!--Supermicro Update Manager 2.7.0 (2021/08/16)-->
  <!--File generated at 2021-08-17_13:34:48-->
  <PhysicalDriveInfo>
    <Information>
      <!--Physical hard drive information, this region is read only.-->
      <DriveCount>2</DriveCount>
      <PhysicalDrive VROCId="25362e54-a291-5a0f-a3e7-71ec761b4838">
        <!--This VROCId is used to identify drive-->
        <DriveStatus>Enabled</DriveStatus>
        <!--Physical drive status, string value-->
        <Temperature>37</Temperature>
        <!--Physical drive temperature in degree C, integer value-->
        <Capacity>2980</Capacity>
        <!--Physical drive capacity in Gigabyte, integer value-->
        <ModelName>INTEL SSDPE2KE032T8</ModelName>
        <!--Physical drive model name, string value-->
        <SerialNumber>PHLN1175029U3P2BGN</SerialNumber>
        <!--Physical drive serial number, string value-->
        <CapableSpeed>32Gb/s</CapableSpeed>
        <!--Physical drive capable speed value, string value-->
        <PredictedFail>false</PredictedFail>
        <!--Physical drive predicted fail, string value-->
      </PhysicalDrive>
      <PhysicalDrive VROCId="bdca9ec7-74db-5d30-8e77-3438be52141a">
        <!--This VROCId is used to identify drive-->
        <DriveStatus>Enabled</DriveStatus>
        <!--Physical drive status, string value-->
        <Temperature>36</Temperature>
```

```
 <!--Physical drive temperature in degree C, integer value-->
      <Capacity>1490</Capacity>
      <!--Physical drive capacity in Gigabyte, integer value-->
      <ModelName>INTEL SSDPE2KE016T8</ModelName>
      <!--Physical drive model name, string value-->
      <SerialNumber>PHLN0355033D1P6AGN</SerialNumber>
      <!--Physical drive serial number, string value-->
      <CapableSpeed>32Gb/s</CapableSpeed>
      <!--Physical drive capable speed value, string value-->
      <PredictedFail>false</PredictedFail>
      <!--Physical drive predicted fail, string value-->
    </PhysicalDrive>
  </Information>
</PhysicalDriveInfo>
<VolumeInfo Action="Change">
  <!--Supported Action:None/Change/ClearAll-->
  <Volume Action="None" VROCId="-1">
    <!--Supported Action:None/Delete/Create-->
    <!--This VROCId is used to identify volume-->
    <Information>
      <Encrypted>false</Encrypted>
      <!--Encryption status of this volume-->
      <BlockSize>0</BlockSize>
      <!--Block size (Bytes), integer value-->
    </Information>
    <Configuration>
      <Name></Name>
      <!--Volume name, string value; length limit = 15 characters-->
      <!--Only used for "Create" action-->
      <Level>RAID0</Level>
      <!--RAID level, string value-->
      <!--Valid value: RAID0/RAID1/RAID5/RAID10-->
```

```
        <!--Only used for "Create" action-->
        <PhysicalDriveList></PhysicalDriveList>
        <!--Physical drive list, string value-->
        <!--Only used for "Create" action-->
        <StripSize>0</StripSize>
        <!--Strip size (KB), integer value-->
        <!--Valid value: -->
        <!--4/8/16/32/64/128 for RAID0-->
        <!--64 for RAID1-->
        <!--4/8/16/32/64/128 for RAID5-->
        <!--4/8/16/32/64/128 for RAID10-->
        <!--Only used for "Create" action-->
        <Capacity>0</Capacity>
        <!--Capacity size (MB), integer value-->
        <!--Only used for "Create" action-->
      </Configuration>
    </Volume>
  </VolumeInfo>
</VROCCfg>
```

- To create a volume:

  Create a RAID 1 volume with both SSDs and "*VROCId*" field should be set to "-1":

  The setting enables a dummy volume table for you to create the volume. Note that for the creation action, "*VROCId*" is meaningless and VROC ID will be generated after the volume is created.

  ```
  <Volume Action="None" VROCId="-1">
        <!--Supported Action:None/Delete/Create-->
        <!--This VROCId is used to identify volume-->
        <Configuration>
          <Name>Dummy</Name>
          <!--Volume name, string value; length limit = 15 characters--
  >
          <!--Only used for "Create" action-->
  ```

```
            <Level>RAID0</Level>
            <!--RAID level, string value-->
            <!--Valid value: RAID0/RAID1/RAID5/RAID10-->
            <!--Only used for "Create" action-->
            <PhysicalDriveList>PHLN0355033D1P6AGN, 25362e54-a291-5a0f-
    a3e7-71ec761b4838</PhysicalDriveList>
            <!--Physical drive list, string value-->
            <!--Only used for "Create" action-->
            <StripSize>64</StripSize>
            <!--Strip size (KB), integer value-->
            <!--Valid value: -->
            <!--4/8/16/32/64/128 for RAID0-->
            <!--64 for RAID1-->
            <!--4/8/16/32/64/128 for RAID5-->
            <!--4/8/16/32/64/128 for RAID10-->
            <!--Only used for "Create" action-->
            <Capacity>1024</Capacity>
            <!--Capacity size (MB), integer value-->
            <!--Only used for "Create" action-->
          </Configuration>
        </Volume>
```

- To delete volume “b8e7131f-a72e-5c2f-a069-977648b74b67”:

```
        <Volume Action="Change" VROCId="b8e7131f-a72e-5c2f-a069-
    977648b74b67">
        </Volume>
```

- To delete all volumes:

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

```
      <VolumeInfo Action="Change">
```

4.13 Remote In-Band Mode

In SUM 2.10.0, you can remotely run in-band commands on a remote system/multiple systems in Remote In-Band mode.

Notes:

- To run commands in this mode, make sure the remote managed system meet the requirements in *1.2.4 In-Band Usage Requirements*.
- In addition, if the remote managed system is FreeBSD, the sudo command must be installed by using "pkg install sudo."
- Since SUM 2.8.1, the RemoteExec command can be used to send files and execute shell commands on a remote system by using the Remote In-Band mode.

4.13.1 Remote SUM and Configurations

To execute Remote In-Band commands on a remote system, the path to the remote SUM executable must be specified. The remote SUM path can be specified in three ways. The priority applies from high to low. Firstly, use the --remote_sum command option to specify the path to the remote SUM executable when executing Remote In-Band commands, which only accept absolute paths. Secondly, rename the remoteSumrc.sample file to ".remoteSumrc," copy it to supermicro/sum_remote_inband under the remote managed system's user home directory, and pre-define the SUM path. See the below example.

```
# set remote SUM path for Remote In-Band usage
remote_sum_path = /root/supermicro/sum_remote_inband/sum
```

If none of the above methods are used, SUM will look for the remote SUM in the default path in supermicro/sum_remote_inband under the user home directory in the remote managed system.

In addition, to execute Remote In-Band commands with customized execution configurations, refer to *4.1 Customizing SUM Configurations*. The only difference is that you use the --remote_rc_file instead of --rc_file if you choose to use the command option to specify the .sumrc file for a remotely managed system.

4.13.2 Using Remote In-Band (Remote_INB) Mode

Syntax:

```
sum -I Remote_INB --oi <OS IP address> -ou <OS user ID> [--op <OS user password>
| -os_key <OS private key> -os_key_pw <OS private key password>] -c <command>
```

Different than the standard in-band operation, entering the username and password of the desired system is required in order to access it remotely.

4.13.3 Using Remote Redfish Host Interface (Remote_RHI)

Syntax:

```
sum -I Remote_RHI -u <username> -p <password> --oi <OS IP address> -ou <OS
username> [--op <OS password> | --os_key <OS private key> --os_key_pw <OS
private key password>] -c <command>
```

For commands or managed systems that require the use of Redfish Host Interface (see *4.10 Redfish Host Interface)*, both the BMC and OS username and password of the remote system are needed.

4.13.4 Console Output

The console output contains the following information when executing Remote In-Band commands. The console output outside the equal signs is SUM that runs the Remote In-Band commands, while the console output inside the equal signs is from the remote managed system.

```
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/17) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.56:
===========================================================================

                Console Output from the Remote Managed System 192.168.34.56
```

```
================================================================================
End Remote In-Band execution on 192.168.34.56.
```

4.13.5 Supported Commands

Currently, the available commands for this usage include:

BIOS Management:

GetBiosInfo, UpdateBios, GetDefaultBiosCfg, GetCurrentBiosCfg, ChangeBiosCfg, LoadDefaultBiosCfg, SetBiosPassword, GetDmiInfo, ChangeDmiInfo, EditDmiInfo, EraseOAKey, BiosRotManage, SecureBootManage

BMC Management:

GetBmcInfo, UpdateBmc, GetBmcCfg, ChangeBmcCfg, GetBmcLANCfg, ChangeBmcLANCfg, SetBmcPassword, GetKcsPriv, GetLockdownMode, LoadDefaultBmcCfg, BmcRotManage, TimedBmcReset, Attestation

Applications:

RemoteExec

Example:

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c
RemoteExec --remote_cmd "ls /tmp/ -l | grep test.sh" --file test.sh
```

Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p Password --oi 192.168.34.57 --ou
root --op 111111 -c GetBmcInfo --remote_sum /root/sum
```

4.13.6 Transferring Files

When executing Remote In-Band commands that involve file transfer, SUM creates a new file (randomly named by 8 characters) in the sum_remote_inband/yyyy-mm-dd_hh-mm-ss folder under the user directory on the remotely managed system for management access. In the meantime, the sum.log file is also created. See *4.2 SUM Log Design* for details. The log file will be saved on the managing system to the remote_inband/yyyy-mm-dd_hh-mm-ss_suffix with an IP address. The below provides an example of running a Remote In-Band command to transfer files with the --file <file> command option.

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
<command> --file <file> --remote_sum /root/sum
```

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/18) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.56:
```

[When the command involves uploading --file <file> to the remote managed system]

```
Sending file '<file>' to '/root/sum_remote_inband/2022-11-18_14-09-
58/hraaqvGG.txt' on 192.168.34.56.

============================================================================
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/14) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.

File "/root/sum_remote_inband/2022-11-18_14-09-58/hraaqvGG.txt" is updated.
============================================================================
```

[When the command involves downloading --file <file> from the remote managed system]

```
Getting file '<file>' from '/root/sum_remote_inband/2022-11-18_14-09-
58/hraaqvGG.txt' on 192.168.34.56.
```

```
Getting file 'remote_inband/2022-11-18_14-10-08_192.168.34.56/sum.log' from
'/root/sum_remote_inband/2022-11-18_14-09-58/sum.log' on 192.168.34.56.

End Remote In-Band execution on 192.168.34.56.
```

4.14 BMC LAN Configuration XML File Format

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

```
<?xml version="1.0"?>
<BmcLANCfg>
  <!--You can remove unnecessary elements so that-->
  <!--their values will not be changed after update-->
  <LAN Action="None">
    <!--Supported Action:None/Change-->
    <Information>
      <!--Information for LAN properties-->
      <SpeedMbps>1000</SpeedMbps>
      <Duplex>Full Duplex</Duplex>
    </Information>
    <Configuration>
      <!--Configuration for LAN properties-->
      <!--Will be skipped in OOB usage mode if BMC doesn't support.-->
      <IPProtocolStatus>Dual</IPProtocolStatus>
      <!--IPv4/IPv6/Dual-->
      <!--The value shall indicate which IP protocol can be accessed.-->
      <LanMode>Share</LanMode>
      <!--Dedicated/Share/Failover-->
      <!--Changing this setting may cause the LAN to be unavailable.-->
      <MacAddr>3C:EC:EF:C6:22:D9</MacAddr>
      <!--X:X:X:X:X:X-->
      <!--Will be skipped in OOB usage mode.-->
      <!--If IPSrc in IPv4 table is DHCP, changing MacAddr will make IPAddr in
IPv4 table change.-->
      <Link></Link>
      <!--Auto Negotiation/10M Half Duplex/10M Full Duplex/100M Half Duplex/100M
Full Duplex-->
      <!--Link can only be updated if LanMode is Dedicated.-->
      <!--Link will be empty if LanMode is Shared.-->
      <!--Will be skipped if empty.-->
      <HostName></HostName>
      <!--BMC host name-->
      <!--string value; length limit = 63 characters-->
      <?Note Will be skipped in multiple system usage without --individually
option.?>
      <CommunityString>public</CommunityString>
      <!--string value; length limit = 18 characters-->
      <VLAN_Enable>Disable</VLAN_Enable>
      <!--Enable/Disable-->
      <!--Changing this setting may cause the LAN to be unavailable.-->
      <VLAN_ID>1</VLAN_ID>
      <!--Integer value is in [1-4094].-->
      <!--0 and 4095 for special purposes.-->
      <!--When VLAN enabled, 0 is prohibited.-->
      <!--When VLAN disabled, value will not be changed.-->
      <!--Changing this setting may cause the LAN to be unavailable.-->
      <RMCP_Port>623</RMCP_Port>
      <!--[1-65535]-->
      <!--In OOB usage, default RMCP port is 623.-->
      <!--If the RMCP port is updated, please configure the 'rmcp_port'
in .sumrc file for OOB BMC connection.-->
      <IPv4 Action="Change">
        <!--Supported Action:None/Change-->
        <Configuration>
          <!--Configuration for IPv4 properties-->
          <!--Will be skipped in OOB usage mode if BMC doesn't support.-->
          <IPSrc>DHCP</IPSrc>
          <!--Static/DHCP-->
          <IPAddr>192.168.34.56</IPAddr>
          <!--X.X.X.X-->
          <!--Each field is an integer in [0-255].-->
          <?Note Will be skipped in multiple system usage without --individually
option.?>
          <SubNetMask>255.255.224.0</SubNetMask>
          <!--X.X.X.X-->
          <!--Each field is an integer in [0-255].-->
          <?Note Will be skipped in multiple system usage without --individually option.?>
          <DefaultGateWayAddr>10.184.7.254</DefaultGateWayAddr>
          <!--X.X.X.X-->
          <!--Each field is an integer in [0-255].-->
          <?Note Will be skipped in multiple system usage without --individually option.?>
          <DNSAddr>1.1.1.1</DNSAddr>
          <!--X.X.X.X-->
          <!--Each field is an integer in [0-255].-->
          <!--Will be skipped if empty.-->
          <DNSAddr2>2.2.2.2</DNSAddr2>
          <!--X.X.X.X-->
          <!--Each field is an integer in [0-255].-->
          <!--DNSAddr2 is read-only.-->
        </Configuration>
      </IPv4>
    </Configuration>
  </LAN>
</BmcLANCfg>
```

- The XML version is shown in the first line.
- The root table name is "*BmcLANCfg*." Its name tag pair is *<BmcLANCfg>* and *</BmcLANCfg>*. All information belonging to the root table is enclosed between this name tag pair.
- 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 the "*<!--*" and "-->" tags. The supported usage of each element and table are shown in its following comments.
- Configuration tables may 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 may contain more table specific attributes if needed.

In this example, the *Action* is *None* for the *LAN* table. As such, SUM will skip updating the element *IPProtocolStatus, LanMode, MacAddr. Link, HostName, CommunityString, VLAN_Enable, VLAN_ID, RMCP_Port* of the table *LAN*. On the other hand, SUM will try to update the value for the *IPSrc* element of the *IPv4* 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*.

4.15 Fixed Boot Configuration XML File Format

The fixed boot configuration is used to power on/off a boot device and to change the boot device order on X13 and later platforms. An example below shows how this file demonstrates the fixed boot configurable elements.

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<FixedBootCfg>
  <!--Supermicro Update Manager 2.10.0 (2022/12/19)-->
  <!--File generated at 2023-01-06_14:30:43-->
  <!--Boot mode selected UEFI-->
  <Menu name="Fixed Boot Order">
    <Setting name="Boot Option #1" selectedOption="UEFI Hard Disk:UEFI OS"
type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI Hard Disk:UEFI OS (SATA,Port:0)</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #2" selectedOption="UEFI CD/DVD" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI CD/DVD</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #3" selectedOption="UEFI USB Hard Disk"
type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB Hard Disk</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #4" selectedOption="UEFI USB CD/DVD"
type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB CD/DVD</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #5" selectedOption="UEFI USB Key" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB Key</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #6" selectedOption="UEFI USB Floppy"
type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB Floppy</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #7" selectedOption="UEFI USB Lan" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB Lan</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #8" selectedOption="UEFI Network:(B4/D0/F0) UEFI
PXE IPv4 Intel(R) Ethernet Controller X550(MAC:3cecefcb33c6)" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #9" selectedOption="UEFI Hard Disk:UEFI OS
(SATA,Port:0)" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI AP:UEFI: Built-in EFI Shell</DefaultOption>
      </Information>
    </Setting>
  </Menu>
  <Menu name="UefiHardDiskBBSPriorities">
```

```
    <Setting name="UEFIHardDisk #1" selectedOption="UEFI OS (SATA,Port:0)"
type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI OS (SATA,Port:0)</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI OS (SATA,Port:0)</DefaultOption>
      </Information>
    </Setting>
  </Menu>
  <Menu name="UefiApplicationBootPriorities">
    <Setting name="UEFIAP #1" selectedOption="UEFI: Built-in EFI Shell"
type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI: Built-in EFI Shell</DefaultOption>
      </Information>
    </Setting>
  </Menu>
  <Menu name="UefiNetworkBBSPriorities">
    <Setting name="UEFINetwork #1" selectedOption="(B4/D0/F1) UEFI PXE IPv4
Intel(R) Ethernet Controller X550(MAC:3cecefcb33c7)" type="Option">
      <Information>
        <AvailableOptions>
          <Option>(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet Controller
X550(MAC:3cecefcb33c6)</Option>
          <Option>(B4/D0/F1) UEFI PXE IPv4 Intel(R) Ethernet Controller
X550(MAC:3cecefcb33c7)</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet Controller
X550(MAC:3cecefcb33c6)</DefaultOption>
      </Information>
    </Setting>
    <Setting name="UEFINetwork #2" selectedOption="(B4/D0/F0) UEFI PXE IPv4
Intel(R) Ethernet Controller X550(MAC:3cecefcb33c6)" type="Option">
      <Information>
        <AvailableOptions>
          <Option>(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet Controller
X550(MAC:3cecefcb33c6)</Option>
          <Option>(B4/D0/F1) UEFI PXE IPv4 Intel(R) Ethernet Controller
X550(MAC:3cecefcb33c7)</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>(B4/D0/F1) UEFI PXE IPv4 Intel(R) Ethernet Controller
X550(MAC:3cecefcb33c7)</DefaultOption>
      </Information>
    </Setting>
  </Menu>
</FixedBootCfg>
```

- The XML version is shown in the first line.
- The root table name is "*FixedBootCfg.*" Its name tag pair is *< FixedBootCfg >* and *</FixedBootCfg >*. All information belonging to the root table is enclosed between this name tag pair.
- There could be several menus in FixedBootCfg, depending on your managed system's boot device.
- Configurable elements are listed in the "*<Setting>*" field of each child table.
- Each name tag pair *<Menu>* encloses name tag pairs *<Menu>*, *<Information>*, *<Setting>*.
- *<Information>* shows the setting-specific information. For example, *<Setting>* with the 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.
- Change setting you can modify after # number or change selectedOption *<Setting name="UEFINetwork #2" selectedOption="(B4/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet Controller X550(MAC:3cecefcb33c6)" type="Option">*
- Comments could be given to the following element or table name tag. Each comment is enclosed by "*<!--*" and "-->" tags.

For more details on usages, refer *Appendix E. How to Change BIOS Configurations in XML Files -E.3 Option*

After changes, save the XML file and then execute the command “ChangeFixedBootCfg” with --reboot option, and the change will take effect after reboot.

Notes:

- Unchanged settings can be deleted to skip the update.
- The XML version line and the *<FixedBootCfg>* root should not be deleted.
- The On/Off boot device can be modified in the *<xxxxxBBSPriorities> <setting>* menu*;* but if the boot device is on the boot order list, you cannot disable it, it should be disabled in boot order first. Later you can disable it in the *<xxxxxBBSPriorities> <setting>* menu.
- If more than one device is listed on the *<xxxxxBBSPriorities> <setting>* menu , you can change the order to change the boot order as well. For example, the two UEFINetwork devices in the “*UefiNetworkBBSPriorities*” menu change their orders after the *"Fixed Boot Order"* menu in *<setting selectedOption=UEFI Network>* option shows the device of the first priority that you change in the “UefiNetworkBBSPriorities” menu. But you cannot change the UEFI Network display device in the *"Fixed Boot Order"* menu directly.
- In FixedBootCfg, ignore the *<WorkIf>* setting because there is no *<WorkIf>* in Configuration.
- For using tools to edit XML files, please refer to *Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files*.

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 Getting 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":"11111111111111111111222222222222223333333333333333ab
abababababababababababbabcdcdcdcdcdccdcdcddcdefefefefefefefeefefefefghghghghghghghghgh"}}'


[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":"11111111111111111111222222222222223333333333333333ab
abababababababababababbabcdcdcdcdcdccdcdcddcdefefefefefefefeefefefefghghghghghghghghgh"}}'
```

```
[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 Getting 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 “QueryProductKey” command.

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 "CheckOOBSupport" command 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 “CheckAssetInfo” command 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 “CheckSensorData” command 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 "CheckSystemUtilization" command 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 "ServiceCalls" command 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.

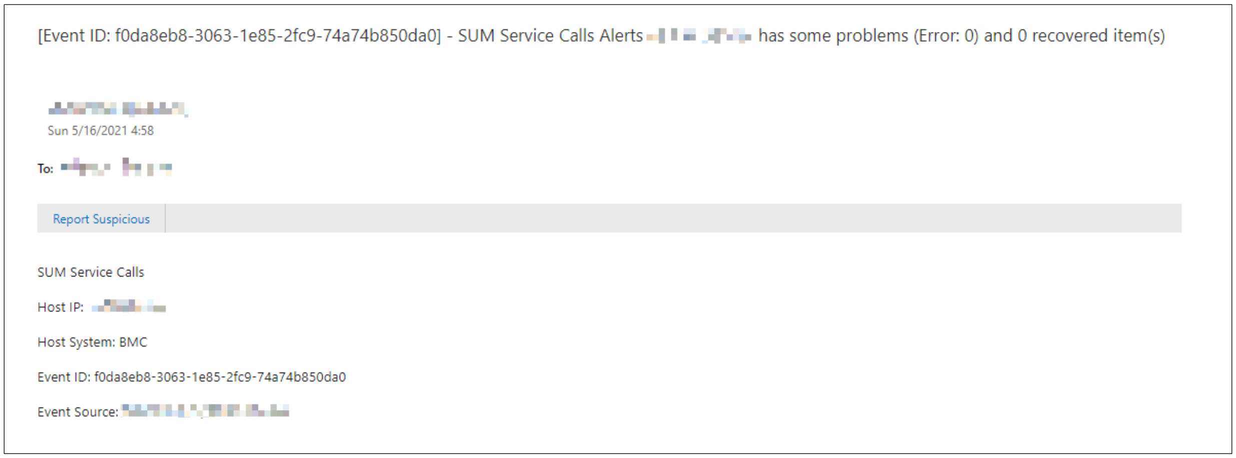
- Site Location Information node - <Site_Location_Information>

  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.

5.2.5.2 Email Format



[Event ID: f0da8eb8-3063-1e85-2fc9-74a74b850da0] - SUM Service Calls Alerts [redacted] has some problems (Error: 0) and 0 recovered item(s)

[redacted]
Sun 5/16/2021 4:58

To: [redacted]

SUM Service Calls

Host IP: [redacted]

Host System: BMC

Event ID: f0da8eb8-3063-1e85-2fc9-74a74b850da0

Event Source: [redacted]

The e-mail content includes:

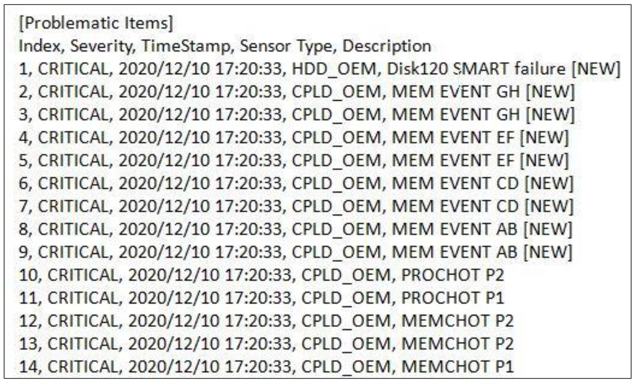
- **Subject Line**

  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 Email**:

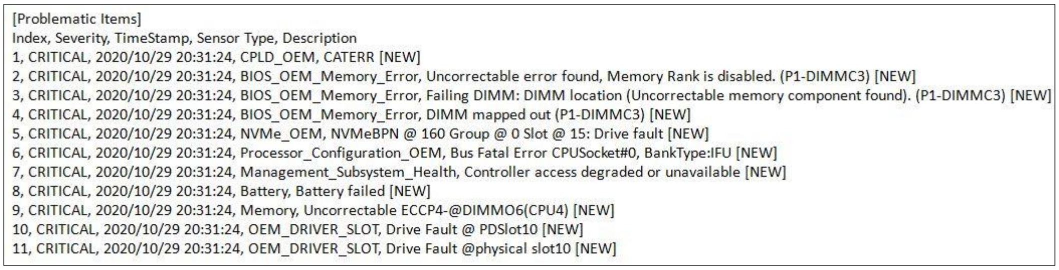
  The SEL problem consists of three severity levels: “critical,” “warning” and “information," which is defined by SUM. The SDR items exceeding their thresholds will be treated as problematic items.



```
[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 Email**:

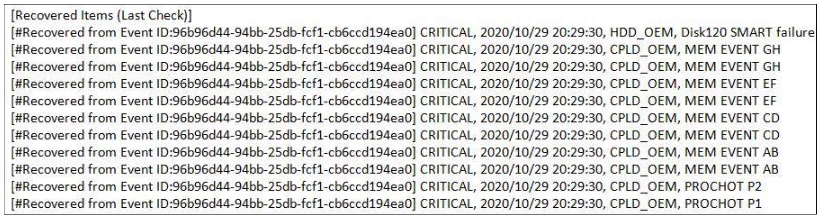
  HW-related events of SEL and SDR all appear as “Critical.”



```
[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)**:

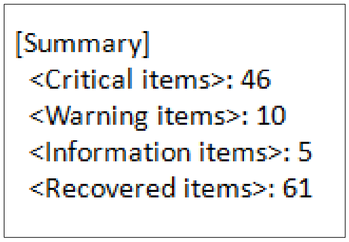
  This section contains the SEL and SDR items previously marked as problematic items but later recovered in the last check.



```
[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.

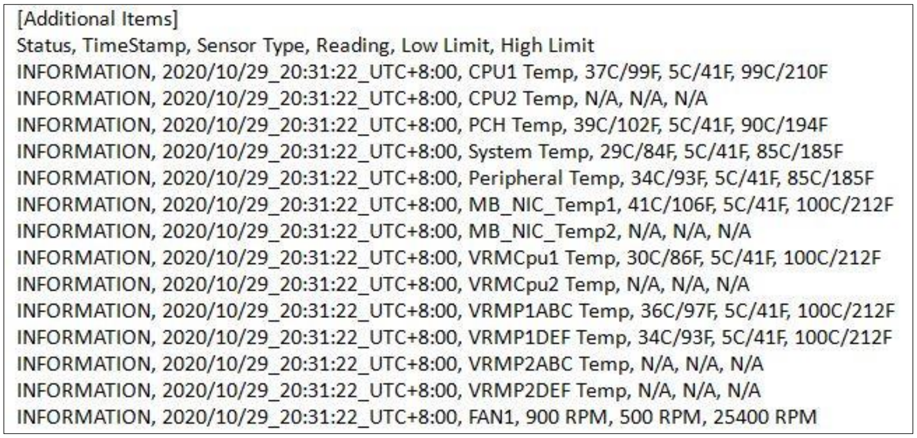


```
[Summary]
 <Critical items>: 46
 <Warning items>: 10
 <Information items>: 5
 <Recovered items>: 61
```

- **Additional Items**:

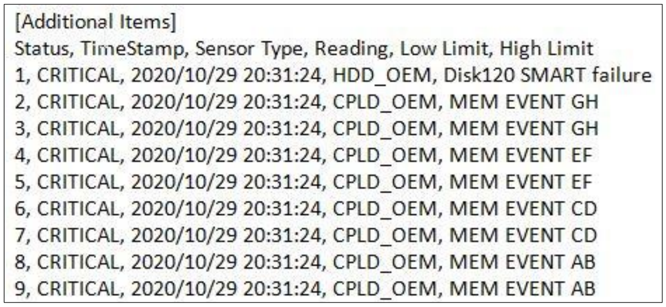
  User-Defined Event Email and HW Event Alert Email are different, but both include status, timestamps, sensor type, reading, and threshold.

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



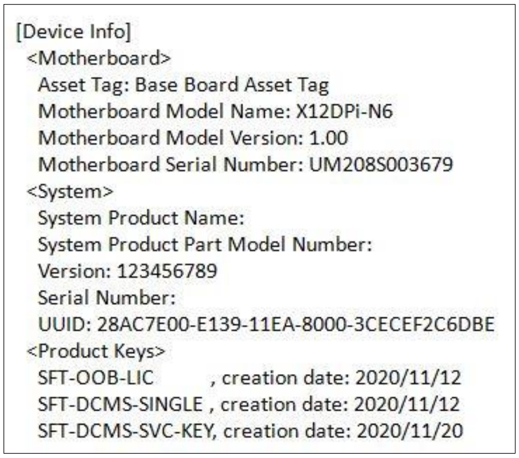
```
[Additional Items]
Status, TimeStamp, Sensor Type, Reading, Low Limit, High Limit
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, CPU1 Temp, 37C/99F, 5C/41F, 99C/210F
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, CPU2 Temp, N/A, N/A, N/A
INFORMATION, 2020/10/29_20:31:22_UTC+8:00, PCH Temp, 39C/102F, 5C/41F, 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 Email**: 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**:

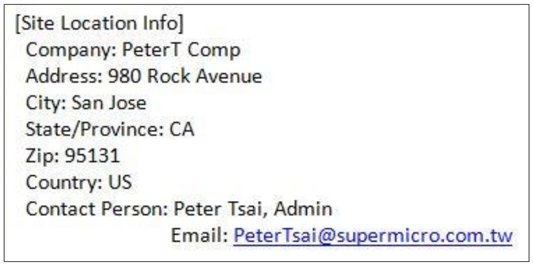


```
[Device Info]
 <Motherboard>
  Asset Tag: Base Board Asset Tag
  Motherboard Model Name: X12DPi-N6
  Motherboard Model Version: 1.00
  Motherboard Serial Number: UM208S003679
 <System>
  System Product Name:
  System Product Part Model Number:
  Version: 123456789
  Serial Number:
  UUID: 28AC7E00-E139-11EA-8000-3CECEF2C6DBE
 <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.

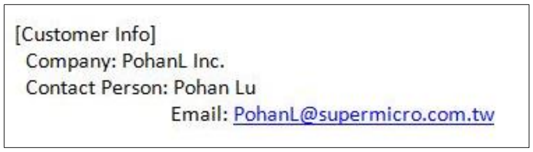
- **Site Location Info**:



```
[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.

5.2.5.3 Cache File

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 is 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.

5.2.6 Monitoring and Controlling PFA of the System

Use the “SystemPFA”command to monitor and set the predictive failure analysis function of BIOS on the managed system.

Syntax:

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

Option Commands	Descriptions
--action	Sets action to: 1 = GetCurrentStatus 2 = Enabled 3 = Disabled

Example:

OOB:

```
1.  [SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SystemPFA --
    action GetCurrentStatus
```

The console output contains the following information.

```
The current system PFA is Disabled
```

```
2.  [SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SystemPFA --
    action Enabled --reboot --post_complete
```

The console output contains the following information.

```
...........

The system PFA is set to Enabled.
```

```
Status: The managed system 192.168.34.56 is rebooting.

..........................Done

Status: The managed system 192.168.34.56 is waiting for POST complete

........................
..................................................
..................................................
..................................................
......
Status: The managed system 192.168.34.56 is POST completed
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c SystemPFA --action
Disabled --reboot
```

Note: This command is only available on X13 platforms.

5.2.7 Checking Memory Health of the Managed System

Use the “MemoryHealthCheck” command to access the function in BIOS to check memory health of the managed system.

Syntax:

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

Option Commands	**Descriptions**
--action	Sets action to: 1 = GetCurrentStatus 2 = Persistent 3 = Enable 4 = Disable

Example:

OOB:

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


The current memory health checking is Disabled


[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MemoryHealthCheck --
action Persistent --reboot --post_complete
```

The console output contains the following information.

```
....
```

```
The memory health checking is set to Persistent.

Status: The managed system 192.168.34.56 is rebooting.

.........................Done

Status: The managed system 192.168.34.56 is waiting for POST complete



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

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

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

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

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

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

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

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

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

Status: The managed system 192.168.34.56 is POST completed



Status: Getting event logs from 192.168.34.56.

ID| Time Stamp |    Sensor Number   |  Sensor Type | Description

18| 01/20/2022 08:33:10 | #0FF (System Firmware Progress) | System Firmware
Progress | Progress: CPU 1 Advanced Memory Test finished
```

```
17| 01/20/2022 08:32:13 | #0FF (System Firmware Progress) | System Firmware Progress | Progress: CPU 1 Advanced Memory Test started
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c MemoryHealthCheck --action Enable --reboot
```

5.2.8 Activating CpuOnDemand

The CpuOnDemand command is designed to support Intel® On Demand Capabilities (abbreviated as IOD) on Intel® Xeon SPR (Sapphire Rapids) and later CPUs and activates additional features during the lifetime of the selected Xeon CPUs. To check if your hardware settings meet the requirements and to learn more about the features, see the DCL [1](Dear Customer Letter) for each SKU in different product bundles.

IOD requires interaction with Supermicro tools and Intel®. The following section describes the flow in general.

5.2.8.1 CpuOnDemand Flow

1. Ensure your CPU[2] is compatible with IOD and run the GeHwInfo command to get hardware information, e.g., PPIN and CPU Socket index.
2. Provide PPIN and system asset information to Supermicro to get a LAC+ file.
   See Table 2 for product features.
3. Apply the LAC+ file and run the SetLicenseActivateCode command to provision CPU.
4. Run the GetOnDemandState command to get a state report file.
5. Send the state report file back to Supermicro in order to send it back to Intel®.

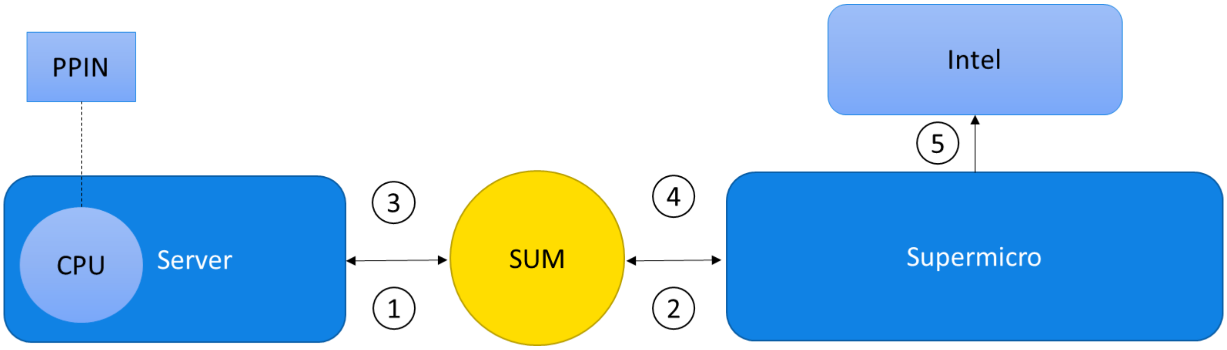
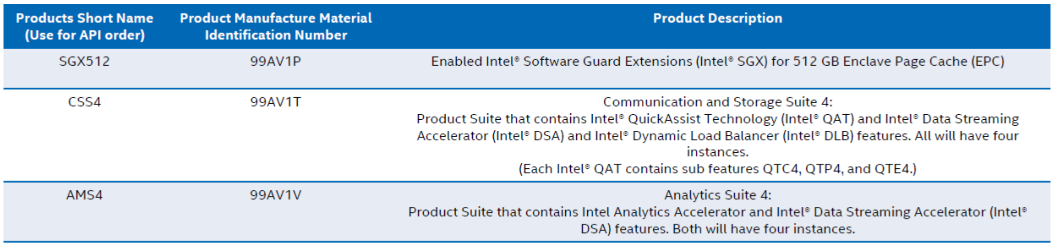


Table 1 - CpuOnDemand Flow

[1] Downloading DCL (Dear Customer Letter) requires an Intel® RDC (Resource & Documentation Center) account.

[2] For On Demand Capabilities-supported CPU SKUs, please contact your sales representative.



Products Short Name (Use for API order)	Product Manufacture Material Identification Number	Product Description
SGX512	99AV1P	Enabled Intel® Software Guard Extensions (Intel® SGX) for 512 GB Enclave Page Cache (EPC)
CSS4	99AV1T	Communication and Storage Suite 4: Product Suite that contains Intel® QuickAssist Technology (Intel® QAT) and Intel® Data Streaming Accelerator (Intel® DSA) and Intel® Dynamic Load Balancer (Intel® DLB) features. All will have four instances. (Each Intel® QAT contains sub features QTC4, QTP4, and QTE4.)
AMS4	99AV1V	Analytics Suite 4: Product Suite that contains Intel Analytics Accelerator and Intel® Data Streaming Accelerator (Intel® DSA) features. Both will have four instances.

Table 2 - SPR Supported Products

5.2.8.2 Using the CpuOnDemand Command

The CpuOnDemand command provides the following actions to collaborate with the On-Demand Capabilities-enabled CPU on the managed system.

Command Options	Descriptions
--action	Sets action to: 1 = GetHwInfo 2 = GetOnDemandState 3 = SetLicenseActivateCode 4 = EnablePPIN

1. Syntax of GetHwInfo:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
CpuOnDemand --action GetHwInfo [--cpu_id <cpu_socket_id>] [--file <
hw_id_file_name>] [--overwrite]
```

Example:

OOB :

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p ADMIN -c CpuOnDemand --action
GetHwInfo --cpu_id 0 --file hwidfile.txt
```

The console output contains the following information.

```
  Hardware type | Index | ID type | Hardware ID       | Vendor         | SDSi
Enabled

    CPU          | 0      | PPIN    | AABBCCDD00112233  | GenuineIntel   |  YES

File "hwidfile.txt" is created.
```

The content of "hwidfile.txt" contains <BMC_MAC>;<CPU_ID>;<PPIN> as below:

```
00:30:48:00:10:12;0;AABBCCDD00112233
```

This file could be used in the GetOnDemandState action with the option of --hw_id_file.

INB:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c CpuOnDemand --action
GetHwInfo --file hwidfile.txt
```

The console output contains the following information.

```
  Hardware type | Index | ID type | Hardware ID       | Vendor    | SDSi Enabled

    CPU          | 0      | PPIN    | AABBCCDD00112233  | GenuineIntel   |  YES

File "hwidfile.txt" is created.cd
```

The content of “hwidfile.txt” contains the following information:

```
00:30:48:00:10:12;0;AABBCCDD00112233
```

2. Syntax of GetOnDemandState:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
CpuOnDemand --action GetOnDemandState [--cpu_id <cpu_socket_id> | --hw_id
<hw_id> | --hw_id_file <hw_id_file_name>] [ [--file <StateReport>] [-v] [--
squash] [--overwrite] | --plain_text ]
```

Example:

OOB:

```
a. [SUM_HOME]# ./sum -I 192.168.34.56 -u ADMIN -p ADMIN -c CpuOnDemand --action
   GetOnDemandState --cpu_id 0 --file StateReport.json
```

The console output contains the following information.

```
Start reading the state report on CPU 0 of 192.168.34.56 system...
.................
State Report has been successfully saved to the file <StateReport__
AABBCCDD00112233.json>.
```

The content of “StateReport__AABBCCDD00112233.json” contains the following information:

```
{
        "hardwareComponentData" :
        [
                {
                        "hardwareId" :
                        {
                                "type" : "PPIN",
                                "value" : "AABBCCDD00112233"
                        },
                        "hardwareType" : "CPU",
                        "stateCertificate" :
                        {
                                "pendingCapabilityActivationPayloadCount" : 0,
                                "value" : “AaaaaBbbbbCcccc"
                        }
                }
        ],
        "objectId" : "496E74656C5F5F5352",
        "syntaxVersion" : "1.0",
        "timestamp" : "2022-09-08T14:16:03+0800"
}
```

```
b. [SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p ADMIN -c CpuOnDemand --action
   GetOnDemandState --cpu_id 0 --file StateReport.txt --squash
```

The console output contains the following information.

```
Start reading the state report on CPU 0 of 192.168.34.56 system...
.................
State Report has been successfully saved to the file <StateReport.txt>.
```

The content of “StateReport.txt” contains the following information:

```
AABBCCDD00112233;{"hardwareComponentData":[{"hardwareId":{"type":"PPIN","value":
"AABBCCDD00112233"},"hardwareType":"CPU","stateCertificate":{"pendingCapabilityA
ctivationPayloadCount":0,"value":"AaaaaBbbbbCcccc”}}],"objectId":"496E74656C5F5F
5352","syntaxVersion":"1.0","timestamp":"2022-09-22T15:28:48+0800"}
```

```
c. [SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p ADMIN -c CpuOnDemand --action
   GetOnDemandState --cpu_id 0 --plain_text
```

The console output contains the following information.

```
Start reading the state report on CPU 0 of 192.168.34.56 system...

NVRAM capacity: 4024 B.
NVRAM used: 292 B (7.26%).

User message:
  - SDSi license auth failure count = 0
  - SDSi license auth failure treshold = 2
  - SDSi license key auth failure = 0
  - SDSi license key auth failure treshold = 2
  - SDSi updates available = 2
  - SDSi updates treshold = 2

Currently active:
  - SGX 512 EPC
```

Active after reboot:

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c CpuOnDemand --action
GetOnDemandState --hw_id AABBCCDD00112233 --file DebugStateReport.json -v
```

The console output contains the following information.

```
Start reading the state report on CPU 0 of 169.254.3.254 system...

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

Debug State Report has been successfully saved to the file <
DebugStateReport.json>.
```

3. Syntax of SetLicenseActivateCode:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
CpuOnDemand --action SetLicenseActivateCode --lac_file <LAC+.txt>] [--reboot] [-
-post_complete]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p ADMIN -c CpuOnDemand --action
SetLicenseActivateCode --lac_file LAC+_ AABBCCDD00112233.txt --reboot
```

The content of “LAC+_ AABBCCDD00112233.txt” contains the following information:

```
AABBCCDD00112233;{"LACPlus":[…]}
```

The console output contains the following information.

```
....
```

```
Start writing new LAC+ file on CPU 1 of 192.168.34.56 system...
...
New LAC+ file has been set successfully and is pending activation.


Status: The managed system 192.168.34.56 is rebooting.


....................................Done
WARNING: Without option --post_complete, please manually confirm the managed
system is POST complete before executing next action.
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c CPUOnDemand --action
SetLicenseActivateCode --lac_file LAC+_AABBCCDD00112233.txt --reboot
```

The console output contains the following information.

```
Start writing new LAC+ file on CPU 0 of 169.254.3.254 system...

...
New LAC+ file has been set successfully and is pending activation.

Status: The managed system 169.254.3.254 is rebooting.

System reboot command issued.
```

4. Syntax of EnablePPIN:

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

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p ADMIN -c CpuOnDemand --action
EnablePPIN --reboot --post_complete
```

Example:

```
The managed system 192.168.34.56 is rebooting.

...

..................................Done

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

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

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

The PPIN Control is set for 192.168.34.56



Status: The managed system 192.168.34.56 is waiting for POST complete

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

Status: The managed system 10.184.16.102 is POST completed
```

INB:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c CpuOnDemand --action
EnablePPIN --reboot
```

5.2.9 Getting and Clearing the Chassis Intrusion Status for the Managed System

Use the “ChassisIntrusion” command to get and clear the status of the chassis intrusion sensor. If a hardware intrusion is detected, the status will be “Hardware Intrusion”. Otherwise, it will be “Normal”. This command can be used to either get the status or set the status to “Normal”.

Syntax:

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

Example:

OOB:

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

The console output contains the following information:

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

    Intrusion Sensor..........Normal
```

In-Band:

```
[SUM_HOME]# sudo ./sum -c ChassisIntrusion --action Clear
```

The console output contains the following information:

```
Chassis intrusion has already been cleared.
```

5.2.10 Managing FRU Information

5.2.10.1 Getting FRU Information

Use the "GetFruInfo" command to get or dump FRU information on the managed system and read FRU information from the local FRU file.

Notes:

- The "--dev_id" option only supports CMM.
- The "--showall" option can support CMM and X13DEG-OAD.

Syntax:

```
sum [-i <IP or host name>] -u <username> -p <password> -c GetFruInfo [--file <filename> [--dump] | [--file_only]] [--overwrite] [--dev_id <Device ID>] | [--showall]
```

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetFruInfo --file dumpedFile --dump --overwrite

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetFruInfo --dev_id 1,2

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

The console output contains the following information:

```
FRU information

===================

    [CMM Master]

        Mfg. Date: 2017/04/05 11:35
        Board Manufacturer: Supermicro

        Board Product Name: Chassis Management Module

        Board Serial Number:

        Board Part Number: MBB-CMM-003

        Manufacturer Name: Supermicro

        Product Name: Chassis Management Module

        Product Part Number: MBM-CMM-003

        Product Version: 1

        Product Serial Number:

        Asset Tag:


    [CMM Middle Plane]

        Mfg. Date: 2017/10/30 14:24

        Board Manufacturer: Supermicro

        Board Product Name: MidPlane

        Board Serial Number: GB196S006132

        Board Part Number: BPN-SB-J610

        Manufacturer Name: Supermicro

        Product Name: MidPlane

        Product Part Number: BPN-SB-J610

        Product Version: 1.00
        Product Serial Number: GB196S006132

        Asset Tag:
```

In-Band:

```
[SUM_HOME]# ./sum -c GetFruInfo --file dumpedFile --file_only
```

The console output contains the following information:

```
Mfg. Date: 2021/08/30 18:01

Board Manufacturer: Supermicro

Board Product Name:

Board Serial Number: WM218S011157

Board Part Number:

Manufacturer Name:

Product Name:

Product Part Number:

Product Version:

Product Serial Number:

Asset Tag:
```

5.2.10.2 Restoring FRU Information

Use the “RestoreFruInfo” command to restore the FRU information on the managed system.

Syntax:

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

OOB:

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

The console output contains the following information:

```
RestoreFruInfo command is Completed.

Mfg. Date: 2021/08/30 18:01

Board Manufacturer: Supermicro

Board Product Name:

Board Serial Number: WM218S011157

Board Part Number:

Manufacturer Name:

Product Name:

Product Part Number:

Product Version:

Product Serial Number:

Asset Tag:
```

In-Band:

```
[SUM_HOME]# ./sum -c RestoreFruInfo --file dumpedFile
```

The console output contains the following information:

```
RestoreFruInfo command is Completed.

Mfg. Date: 2021/08/30 18:01

Board Manufacturer: Supermicro
Board Product Name:

Board Serial Number: WM218S011157

Board Part Number:

Manufacturer Name:

Product Name:

Product Part Number:

Product Version:

Product Serial Number:

Asset Tag:
```

5.2.10.3 Changing FRU Information

Use the “ChangeFruInfo” command to change the FRU information on the managed system.

Syntax:

```
sum [-i <IP or host name>] -u <username> -p <password> -c ChangeFruInfo --item
<item name> --value <assignment value>
```

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeFruInfo --item
CT --value 0x01
```

The console output contains the following information:

```
ChangeFruInfo command is completed.

Chassis Type: 01

Chassis Part Number:

Chassis Serial Number:
```

```
Mfg. Date: 2021/08/30 18:01

Board Manufacturer: Supermicro

Board Product Name:

Board Serial Number: WM218S011157

Board Part Number:

Manufacturer Name:

Product Name:

Product Part Number:

Product Version:

Product Serial Number:

Asset Tag:
```

In-Band:

```
[SUM_HOME]# ./sum -c ChangeFruInfo --item CT --value 0x01
```

The console output contains the following information:

```
ChangeFruInfo command is completed.

Chassis Type: 01

Chassis Part Number:

Chassis Serial Number:

Mfg. Date: 2021/08/30 18:01

Board Manufacturer: Supermicro

Board Product Name:
```

```
Board Serial Number: WM218S011157

Board Part Number:

Manufacturer Name:

Product Name:

Product Part Number:

Product Version:

Product Serial Number:

Asset Tag:
```

5.3 Managing a Single System

5.3.1 Getting BIOS Firmware Image Information

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

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum [-I Remote_INB | -I Remote_RHI -u <username> -p <password>] --oi <OS IP
address> --ou <OS username> [--op <OS password> | --os_key <OS private key>
--os_key_pw <OS private key password>] -c GetBiosInfo [--file <filename> [--
file_only]] [--showall] [--extract_measurement] [--remote_sum <remote sum path>]
```

Example:

OOB:

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

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

```
Managed system...........192.168.34.56
    Board ID.............0660
    BIOS build date......2012/10/17
Local BIOS image file.... Supermicro_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 Supermicro_BIOS_signed.rom --file_only
```

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

```
Local BIOS image file....Supermicro_BIOS_signed.rom
    Board ID.............1B6A
    BIOS build date......2021/01/12
    FW image.............Signed
        Signed Key.......RoT
```

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

The console output contains the following information.

```
Managed system:
    Board ID.............0660
    BIOS build date......2012/10/17
    BIOS version.........1.0
    BIOS revision........1.8
Local BIOS image file....Supermicro_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
```

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

The console output contains the following information.

```
Local BIOS image file...................Supermicro_BIOS.rom

    Board ID............................1B6A

    BIOS build date.....................2022/05/27

    FW image............................Signed

        Signed Key......................RoT

        Measurement.....................FB0DC09383104F49834E2E903F46F365259CB598
6D97F0F3D9DB5945E0D0DFD59F8511F6857E915B414A1B9A30071EF5D99018144033DCC80464B951
E555402B
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c
GetBiosInfo --remote_sum /root/sum
```

Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.57 --ou
root --op 111111 -c GetBiosInfo --remote_sum /root/sum
```

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/02) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.57:
================================================================================
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/02) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.
Reading BIOS flash ..................... (100%)
Managed system:
    Board ID............................1A07
    BIOS build date.....................2021/05/25
================================================================================

Getting file 'remote_inband/2022-11-03_17-38-55_192.168.34.57/sum.log' from
'/root/sum_remote_inband/2022-11-03_17-37-49/sum.log' on 192.168.34.57.

End Remote In-Band execution on 192.168.34.57.
```

The SecureFlash-signed key of the 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 by Super Micro Computer, Inc., but an unknown authority.
(Not shown)	The “FW image” field is not shown because of no secure flash being signed in the image.

A RoT-signed key of the 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.

5.3.2 Updating the BIOS Firmware Image

Use the “UpdateBios” command with the BIOS firmware image Supermicro_BIOS.rom or bios_image.tar for OpenBMC to run SUM to update the managed system.

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum [-I Remote_INB | -I Remote_RHI -u <username> -p <password>] --oi <OS IP
address> --ou <OS username> [--op <OS password> | --os_key <OS private key>
--os_key_pw <OS private key password>] -c UpdateBios --file <filename> [--
remote_sum <remote sum path>] [options…]
```

Option Commands	Descriptions
--reboot	Forces the managed system to reboot or power up after operation.
--flash_smbios	Overwrites and resets the SMBIOS data.
--preserve_mer	Preserves the ME firmware region.
--preserve_nv	Preserves the NVRAM.
--kcs	Updates BIOS through KCS. (Support is available on platforms before X11 with OEM BMC request only and can be only used with in-band usage.)
--preserve_setting	Preserves BIOS configurations.
--erase_OA_key	Erases the OA key.
--backup	Backs up the current BIOS image. (Only supported by RoT systems.)
--forward	Confirms the Rollback ID and upgrades to the next revision. (Only supported by X12/H12 and later platforms except for H12 non-RoT systems.)
--staged <action>	Sets action to: 1 = update: The Update process will start at the next system boot. 2 = abort: Aborts the previous staged update task. 3 = getinfo: Check if there was any pending staged update task.
--post_complete	Waits for the managed system POST to complete after reboot.
--clear_password	Clears the BIOS password.
--erase_secure_boot_key	Erases the secure boot key.
--reset_boot_option	Resets the BIOS boot configurations.

Notes:

- Before performing the OOB UpdateBios command, it is recommended to shut down the managed system first.
- When performing an in-band UpdateBios command, SUM will disable watchdog and unload the 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 “UpdateBios” in-band SUM command 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 an SSH connection to run the UpdateBios in-band command, the SSH timeout on both the client and server sides should be adjusted to avoid a 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 UpdateBios in-band command is executed, a warning message stating the necessary actions is displayed.
- When multiple boots are installed, use the 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.
- Signed BIOS update is supported.
- X12/H12 RoT platforms support staged update only if both BMC and CPLD support it as well.
- For some X12/H12 RoT platforms, BIOS can only be updated while the system is powered off. In this case, the --reboot option is required. Therefore, for in-band BIOS updates, SUM will power off the system after uploading BIOS image to start the update process. The system will be powered on automatically after the BIOS update has completed.
- For X12/H12 and later RoT platforms, in-band BIOS updates can only be done through the Redfish Host Interface. For details, refer to *4.10 Redfish Host Interface*.
- The --backup option backs up the current BIOS image on the managed system, not the BIOS file to be updated.
- The --backup option is only supported by X12/H12 and later RoT platforms.
- Due to a known GRUB2 loader issue, the system may not be able to boot and may hang up after BIOS update is upgraded. If the o GRUB2 loader version is not the lastest, please downgrade the BIOS to the previous version and upgrade the GRUB2 loader to the latest version. Then perform a BIOS upgrade to the target BIOS again. For more details, please refer to the FAQ on the Supermicro website https://www.supermicro.com/support/faqs/faq.cfm?faq=33400.
- OpenBMC only accepts tar firmare files for BIOS firmware updates. Please refer to the

appendix *L.1 BIOS Firmware Updating Tar File for OpenBMC* for creating a tar file firmware image.

Example:

OOB:

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

In-Band:

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

In-Band through KCS:

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

In-Band through Redfish Host Interface:

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

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
UpdateBios --file Supermicro_BIOS.rom --reboot --remote_sum /root/sum
```

Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 --ou
root --op 111111 -c UpdateBios --file Supermicro_BIOS.rom --reboot --remote_sum
/root/sum
```

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 the BIOS and BMC firmware images at the same time.
- The --preserve_nv and --flash_smbios options cannot be used at the same time.
- The --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.
- The --preserve_nv option is used to preserve BIOS NVRAM data. Unless you are familiar with BIOS NVRAM, do not use this option.
- The --preserve_mer option is used to preserve the ME firmware region. Unless you are familiar with the ME firmware region, do not use this option.
- The --preserve_setting option requires an 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 GetCurrentBioscfg and GetDefaultBioscfg commands after BIOS is updated. Compare the two files and the different values between these two files are the preserved settings.
- Firmware verification to update the BMC is supported. SUM prevents the BMC from being updated with unauthorized firmware.
- In-band usage through KCS is only supported on non-Redfish platforms (before X11 platforms) with an OEM BMC request only. It is not generally supported on a standard BMC.

5.3.3 Getting Current BIOS Settings

Use the “GetCurrentBiosCfg” command to execute SUM to get the current BIOS settings from the managed system and save it in the 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 the 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 the BIOS configuration contains extended ASCII characters. Please use ISO 8859-1 encoding to view the BIOS configuration XML file.
- SUM 2.2.0 or later supports text-based user interface (TUI). For details, refer to *4.9 TUI.*

- SUM 2.7.0 or later supports generating a compact version of the BIOS configuration file for TUI using the "--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*.
- TUI does not support Remote In-band usage.

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
GetCurrentBiosCfg --file <USER_SETUP.file> [[--current_password <current
password>] | [--cur_pw_file <current password file path>]] [--overwrite] [--
remote_sum <remote sum path>]
```

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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
GetCurrentBiosCfg --file USER_SETUP.file --overwrite --remote_sum /root/sum
```

5.3.4 Updating BIOS Settings Based on the Current BIOS Settings

1. Follow the steps in *5.3.3 Getting 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 "ChangeBiosCfg" command 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 --skip_bbs option 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 identification.

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> [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [--reboot]
```

Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
ChangeBiosCfg --file <USER_SETUP.file> [[--current_password <current password>]
| [--cur_pw_file <current password file path>]] [--reboot] [--remote_sum <remote
sum path>]
```

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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
ChangeBiosCfg --file USER_SETUP.file --reboot --remote_sum /root/sum
```

5.3.5 Getting Factory BIOS Settings

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

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
GetDefaultBiosCfg --file <USER_SETUP.file> [[--current_password <current
password>] | [--cur_pw_file <current password file path>]] [--overwrite] [--
remote_sum <remote sum path>]
```

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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111-c
GetDefaultBiosCfg --file USER_SETUP.file --overwrite --remote_sum /root/sum
```

5.3.6 Updating BIOS Settings Based on the Factory Settings

1. Follow the steps in 5.3.5 Getting 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 “LoadDefaultBiosCfg“ command 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.

OOB and In-Band Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c LoadDefaultBiosCfg [[--current_password <current password>] | [--cur_pw_file <current password file path>]] [--reboot]
```

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> | --os_key <OS private key> --os_key_pw <OS private key password>] -c LoadDefaultBiosCfg [[--current_password <current password>] | [--cur_pw_file <current password file path>]] [--reboot] [--remote_sum <remote sum path>]
```

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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
LoadDefaultBiosCfg --reboot --remote_sum /root/sum
```

5.3.8 Getting DMI Information

Use the “GetDmiInfo” command 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 a 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.

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c GetDmiInfo -
-file <DMI.txt> [--overwrite] [--remote_sum <remote sum path>]
```

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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
GetDmiInfo --file DMI.txt --overwrite --remote_sum /root/sum
```

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 Getting DMI Information* to get 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 get a DMI.txt file, follow the steps in *5.3.8 Getting DMI Information*.

Syntax:

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c EditDmiInfo
--file <DMI.txt> [--item_type <Item Type> --item_name <Item Name> | --shn <Item
Short Name>] [--value <Item Value> | --default] [--remote_sum <remote sum path>]
```

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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
EditDmiInfo --file DMI.txt --shn SYVS --value 1.01 --remote_sum /root/sum
```

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 "ChangeDmiInfo" command 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.

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
ChangeDmiInfo --file <DMI.txt> [--reboot] [--remote_sum <remote sum path>]
```

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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
ChangeDmiInfo --file DMI.txt --reboot
```

5.3.11 Setting Up BIOS Action

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

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
SetBiosPassword [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [[--new_password <new password> --
confirm_password <confirm password>] | [--pw_file <password file path>]] [--
reboot] [--remote_sum <remote sum path>]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBiosPassword
--new_password 123456 --confirm_password 123456 --current_password 654321 --
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 --cur_file
cur_passwd.txt --reboot
```

```
passwd.txt:

    BiosPassword

cur_passwd.txt

    CurBiosPassword
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
SetBiosPassword --new_password 123456 --confirm_password 123456 --reboot --
remote_sum /root/sum

[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
SetBiosPassword --pw_file passwd.txt --cur_file cur_passwd.txt --reboot --
remote_sum /root/sum

passwd.txt:

    BiosPassword

cur_passwd.txt

    CurBiosPassword
```

Notes:

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

5.3.13 Erasing the BIOS OA Key

Use the “EraseOAKey” command 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.
- This command only supports in-band usage.

In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c EraseOAKey
[--reboot] [--remote_sum <remote sum path>]
```

Example:

In-Band:

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

Remote In-Band:

```
 [SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
EraseOAKey --reboot --remote_sum /root/sum
```

5.3.14 Managing BIOS RoT Functions

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

- **Getting Information on BIOS**

  Use the “BiosRotManage” command with the “--action GetInfo” option to retrieve information on active BIOS, backed-up BIOS and Golden BIOS.
- **Updating the Golden BIOS Image**

  Use the “BiosRotManage” command with the “--action UpdateGolden” option to replace the Golden image with an active BIOS image.
- **Recovering BIOS**

  Use the “BiosRotManage” command with the “--action Recover” option 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.
- **Downloading BIOS Evidence**

  Use the “BiosRotManage” command with the “--action DownloadEvidence” option to download BIOS evidence.

Notes:

- To execute the “UpdateGolden” or “Recover” commands, it is necessary to power off a system, and requires the --reboot option.
- 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 “Recover” and “DownloadEvidence” commands, 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.
- The “DownloadEvidence” action is only available after automatic or manual BIOS recovery.
- The BIOS evidence is a compressed gzip file.

OOB and In-Band Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
BiosRotManage --action <action> [--file <evidence.bin.gz>] [--overwrite] [--
reboot]
```

Remote In-Band Syntax:

```
sum -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS
username> [--op <OS password> | --os_key <OS private key> --os_key_pw <OS
private key password>] -c BiosRotManage --action <action> [--file
<evidence.bin.gz>] [--overwrite] [--reboot] [--remote_sum <remote sum path>]
```

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.
..................................................
..................................................
..................................................
.............
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c BiosRotManage --
action DownloadEvidence --file evidence.bin.gz
```

The console output contains the following information.

```
.....

Start generating BIOS evidence.
```

```
....................Done

Start downloading BIOS evidence...........Done

BIOS evidence file "evidence.bin.gz" is created.
```

In-Band through Redfish Host Interface:

```
[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
```

Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 --ou
root --op 111111 -c BiosRotManage --action GetInfo --remote_sum /root/sum
```

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/09) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.56:
================================================================================
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/07) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.

Managed system.....................192.168.34.57
    BIOS build date................2022/10/24 Ver 1.0a
    Backup BIOS build date.........2022/10/24 Ver 1.0a
    Golden BIOS build date.........2022/10/24 Ver 1.0a
=================================================================================

Getting file 'remote_inband/2022-11-09_13-37-10_192.168.34.56/sum.log' from
'/root/sum_remote_inband/2022-11-09_13-37-05/sum.log' on 192.168.34.56.

End Remote In-Band execution on 192.168.34.56.
```

5.3.15 Seamless Update Capsule File

On Seamless-supported platforms, BIOS firmware image format is a combination of many parts of capsule block. With the Seamless Update feature, you can update only one or some parts of capsule block seamlessly, without the complete updating process.

Notes:

- Seamless Update feature only supported on X13 RoT platform or later.
- This command is only available on SUM 2.9.0 or later.

- **Seamless Update Feature in UpdateBios Command**

OOB and In-Band Syntax:

```
sum <-i <IP or host name> | -I Redfish_HI> -u <username> -p <password> -c
UpdateBios --file <CAPSULE_FILE.bin> [--staged update] [--reboot] [--
post_complete]
```

Remote In-Band Syntax:

```
sum -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS
username> [--op <OS password> | --os_key <OS private key> --os_key_pw <OS
private key password>] -c UpdateBios --file <CAPSULE_FILE.bin> [--staged update]
[--reboot] [--post_complete] [--remote_sum <remote sum path>]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBios --file
CAPSULE_FILE.bin --reboot --post_complete
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -c UpdateBios --file CAPSULE_FILE.bin
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 --ou
root --op 111111 -c UpdateBios --file CAPSULE_FILE.bin --remote_sum /root/sum
```

Updating a capsule file employs the same command as updating a full BIOS file. There are certain rules to keep in mind while using this function:

1. There is anti-rollback mechanism to prevent users from downgrading capsule files based on the package versions.
2. If users see the "layout ID mismatch" error message, it means that users need to update the full BIOS image that has the same layout ID with the desired capsule to update into the motherboard.
3. If users see the "Invalid Capsule file" error message, users need to get the correct capsule file designed for that specific platform type, such as: capsule designed for X13 can't be used on other platforms.
4. Some options will be ignored when updating a capsule file, including --backup, --preserve_setting, --flash_smbios, --erase_OA_key, --clear_password, --erase_secure_boot_key, and --reset_boot_option.

- **Getting capsule information in GetBiosInfo command**

OOB and In-Band Syntax:

```
sum <-i <IP or host name> | -I Redfish_HI> -u <username> -p <password> -u
<username> -p <password> -c GetBiosInfo --file <CAPSULE_FILE.bin> [--showall]
```

Remote In-Band Syntax:

```
sum -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS
username> [--op <OS password> | --os_key <OS private key> --os_key_pw <OS
private key password>] -c GetBiosInfo --file <CAPSULE_FILE.bin> [--showall]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBiosInfo --file
CAPSULE_FILE.bin --showall
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -c GetBiosInfo --file CAPSULE_FILE.bin
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
GetBiosInfo --file CAPSULE_FILE.bin
```

Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p ADMIN --oi 192.168.34.56 --ou root -
-op 111111 -c GetBiosInfo --file CAPSULE_FILE.bin
```

You can get capsule information using GetBiosInfo command with input capsule file. Besides, when motherboard support Seamless Update (X13 or later platform), you can also get all the capsule blocks information on managed system by using the `--showall` option. You can have some variation outputs by:

1. Executing the GetBiosInfo command with the --file CAPSULE_FILE.bin --file_only options will show capsule information of the local file.
2. Executing the GetBiosInfo command with the --file BIOS_FILE.bin --showall --file_only options will show all the capsule information supported by the current local BIOS file.
3. Executing the GetBiosInfo command in OOB or in-band Redfish_HI mode with the --file CAPSULE _FILE.bin option on the managed system should show the corresponding capsule information on managed system.
4. Executing the GetBiosInfo command in OOB or in-band Redfish_HI mode with the --showall option on the managed system should show all types of capsule information supported by managed system.

5.3.16 Getting SCP Firmware Image Information

Use the “GetScpInfo” command to get the SCP firmware image information from the managed system.

Syntax:

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

Example:

OOB:

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

The console output contains the following information.

```
Managed system..........................192.168.34.56
        SCP version.....................2.0a
```

In-Band:

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

The console output contains the following information.

```
Managed system..........................169.254.3.254
        SCP version.....................2.0a
```

5.3.17 Updating the SCP Firmware Image

Use the “UpdateScp” command with SCP firmware image scp_image.tar to run SUM to update the managed system.

Notes:

- BMC only accepts the tar firmware file for SCP firmware updates. To creating a .tar firmware image, refer to the *A*ppendix *L.2 Ampere SCP Firmware Updating Tar File for OpenBMC*.
- When using an SSH connection to run the UpdateScp in-band command, the SSH timeout on both client and server side should be adjusted to avoid a broken pipe during command execution. Typical execution time is within 30 minutes. Timeout value should be longer than 30 minutes.
- SCP can only be updated while the system is powered off. In this case, the --reboot option is required. Therefore, for in-band SCP updates, SUM will power off the system after uploading an SCP image to start the update process. The system will be powered on automatically after the SCP update is completed.
- In-band SCP updates can only be done through the Redfish Host Interface. For details, refer to *4.10 Redfish Host Interface*.

Syntax:

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

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateScp --file
scp_image.tar --reboot
```

The console output contains the following information.

```
Managed system.....................192.168.34.56
    SCP FW version.................2.0a
Local SCP image file...............scp_image.tar
Status: Start updating SCP for 192.168.34.56
```

```
************************************WARNING*************************************
    Do not remove AC power from the server.
********************************************************************************

Powering off target system............Done

Uploading FW...Done
Updating FW.....................................................
............Done

Powering up target system............Done

Status: SCP is updated for 192.168.34.56
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateScp --file
scp_image.tar --reboot
```

The console output contains the following information.

```
Managed system.....................169.254.3.254
    SCP FW version.................2.0a
Local SCP image file...............scp_image.tar
Status: Start updating SCP for 169.254.3.254

************************************WARNING*************************************
    Do not remove AC power from the server.
********************************************************************************

Uploading FW...Done
```

```
Note: System will be powered off shortly to continue the update process.
Warning: Please wait for the system to power on again. This may take several
minutes. Do not remove AC power before system reboot.
```

5.3.18 Getting Fixed Boot Setting

Use the “GetFixedBootCfg” command to get the fixed boot order configuration of the managed system.

- **Note:** The Get Fixed Boot Configuration command only supports X13 platforms or later.

OOB and In-Band Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
GetFixedBootCfg [--file <filename>] [--overwrite] --redfish
```

Example:

OOB:

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

--redfish --file FixedBootCfg.xml --overwrite
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c GetFixedBootCfg --redfish

--file FixedBootCfg.xml --overwrite
```

5.3.19 Updating the Fixed Boot Setting

1. Follow the steps in *5.3.18 Getting Fixed Boot Setting*.

2. Edit the item/variable values in the user setup text file USER_SETUP.file to the desired values as illustrated in *4.15 Fixed Boot Configuration XML File Format*.

3. Use the "ChangeFixedBootCfg" command with the updated file USER_SETUP.file to run SUM to update the Fixed Boot configuration.

Notes:

- Unchanged settings can be deleted to skip the update.
- The XML version line and the *<FixedBootCfg>* should not be deleted.
- The On/Off boot device can be modified in the <xxxxxBBSPriorities> <setting> menu, but if the boot device is on the boot order list you cannot disable it. You need to change the BBSPriorities for the device and then you can disable it in the menu <xxxxxBBSPriorities> <setting>.
- If more than one device is listed on the menu *<xxxxxBBSPriorities> <setting>*, you can change the order to change the boot order list. For example, two UEFINetwork devices in the "*UefiNetworkBBSPriorities*" menu change their orders after the *"Fixed Boot Order"* menu in the *<setting selectedOption=UEFI Network>* option shows the device of first priority that you change in the "UefiNetworkBBSPriorities" menu. But you cannot change UEFI Network display device in the*"Fixed Boot Order"* menu directly.
- The change will take effect after the managed system is rebooted.

Syntax:

```
sum [-i <IP or host name>| -I Redfish_HI -u <username> -p <password>] -c
ChangeFixedBootCfg --file <USER_SETUP.file> [--reboot] --redfish
```

Example:

OOB:

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

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c ChangeFixedBootCfg --
redfish --file USER_SETUP.file --reboot
```

5.3.20 Managing Secure Boot

Use the “SecureBootManage” command to manage secure boot. This command can be used to get or set secure the boot status to “Enabled/Disabled,” and it can be also used to upload or delete secure boot keys.

- **Getting secure boot status**

  Use the “SecureBootManage” command with the “--action Status” option to get system secure boot status from BMC Redfish API.

- **Setting secure boot status**

  Use the “SecureBootManage” command with the “--action Enable/Disable” option to set system secure boot pending status through BMC Redfish API. This requires a system reboot to take effect.

- **Showing databases**

  Use the “SecureBootManage” command with the “--action ShowDatabases” option and “--file_type ” option to get the information of specified system secure boot keys through BMC Redfish API. Without “--file_type ” option, it will show the number of all system secure boot keys.

- **Uploading certificate:**

  Use the “SecureBootManage” command with the “--action UploadCertificate” option, “--file_type ” option and “--file” option to upload system secure boot key through BMC Redfish API.

- **Reseting all keys to default**

  Use the “SecureBootManage” command with the “--action ResetAllKeysToDefault” option to reset all system secure boot keys to default through BMC Redfish API.

- **Deleting all keys**

  Use the “SecureBootManage” command with the “--action DeleteAllKeys” option to delete all keys of system secure boot through BMC Redfish API.

- **Deleting PK**

  Use the “SecureBootManage” command with the “--action DeletePK” option to delete PK of system secure boot through BMC Redfish API.

Notes:

- This command is only available on X13/H13 and later platforms.

- 2020.3 Redfish schema.
- The SFT-DCMS-SINGLE license is required.
- This command is only available for Redfish usage.
- You have to reboot or power up the system for the BIOS changes to take effect.
- The argument of “--file_type” option is “PK,” “KEK,” “db,” “dbr,” “dbt” or “dbx” (case sensitive).
- The “--file” option” only supports PEM files.

OOB and In-Band Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
SecureBootManage --redfish --action <action> [--file_type <file type>] [--file
<CertificateFile>] [--reboot [--post_complete]]
```

Remote In-Band Syntax:

```
sum -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS
username> [--op <OS password> | --os_key <OS private key> --os_key_pw <OS
private key password>] -c SecureBootManage --redfish --action <action> [--
file_type <file type>] [--file <CertificateFile>] [--reboot [--post_complete]]
[--remote_sum <remote sum path>]
```

Example:

OOB :

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureBootManage --
redfish --action Enable
```

The console output contains the following information.

```
....

Status: Secure boot has already been enabled.

Note: You have to reboot or power up the system for the BIOS changes to take
effect.
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SecureBootManage --
redfish --action UploadCertificate --file_type KEK --file CertificateFile.pem
```

The console output contains the following information.

```
Status: Certificate has already been uploaded.

Note: You have to reboot or power up the system for the BIOS changes to take
effect
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c SecureBootManage --
redfish --action ShowDatabases
```

The console output contains the following information.

```
.......

Managed system...........................10.184.16.102
    Number of Platform Keys(PK)...........1
    Number of Key Exchange Keys(KEK)......0
    Number of Authorized Signatures(db)...0
    Number of OS Recovery Signatures(dbr).0
    Number of Authorized Timestamps(dbt)..0
    Number of Forbidden Signatures(dbx)...0
```

Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 --ou
root --op 111111 -c BiosRotManage --action GetInfo --remote_sum /root/sum
```

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.11.0 (2023/04/12) (x86_64)
Copyright(C) 2013-2023 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.56:
```

```
=================================================================================
Supermicro Update Manager (for UEFI BIOS) 2.11.0 (2023/04/12) (x86_64)
Copyright(C) 2013-2023 Super Micro Computer, Inc. All rights reserved.
....
Managed system................192.168.34.57
    Secure boot status........Disabled
=================================================================================

Getting file 'remote_inband/2023-04-12_13-37-10_192.168.34.56/sum.log' from
'/root/sum_remote_inband/2023-04-12_13-37-05/sum.log' on 192.168.34.56.

End Remote In-Band execution on 192.168.34.56.
```

5.4 BMC Management for a Single System

5.4.1 Getting BMC Firmware Image Information

Use the “GetBmcInfo” command to get the BMC firmware image information from the managed system as well as the BMC firmware image.

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum [-I Remote_INB | -I Remote_RHI -u <username> -p <password>] --oi <OS IP
address> --ou <OS username> [--op <OS password> | --os_key <OS private key> --
os_key_pw <OS private key password>] -c GetBmcInfo [--file <filename> [--
file_only] [--extract_measurement] [--remote_sum <remote sum path>]
```

Example:

OOB:

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

In-Band:

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

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

```
Managed system............localhost
    BMC type..............X11_ATEN_AST2500_2
    BMC version...........12.63.00
    BMC ext. version......01 00 00
Local BMC image file......Supermicro_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 Supermicro_ROT_BMC.rom --file_only
```

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

```
Local BMC image file...... Supermicro_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
```

```
[SUM_HOME]# ./sum -c GetBmcInfo --file Supermicro_ROT_BMC.rom --file_only --
extract_measurement
```

The console output contains the following information.

```
Local BMC image file.....BMC_X12AST2600-ROT-6202MS_20220624_01.02.33_STDsd.bin
    BMC UFFN.............BMC_X12AST2600-ROT-6202MS_20220624_01.02.33_STDsd.bin
    BMC type.............X12_RoT_ATEN_AST2600_2
    BMC version..........01.02.33
    BMC build date.......2022/06/24
    FW image.............Signed
        Signed Key.......RoT
        Measurement......CE772709B937E6F256A09B9CEDFB9F7F4195B19143543964FD00C90
0BD73F1F36743724B34392B06D4D1D5542CFA0619C32AF960B93A3973A4F2101762A8698D
[SUM_HOME]# ./sum -c GetBmcInfo --file Supermicro ROT BMC.rom --showall
```

The console output contains the following information.

```
Local BMC image file..... BMC_X12AST2600-ROT-5201MS_20230204_09.20.72_BETsp.bin
    BMC UFFN.............BMC_X12AST2600-ROT-5201MS_20230204_09.20.72_BETsp.bin
    BMC type.............X12_RoT_ATEN_AST2600
    BMC version..........09.20.72
    BMC ext. version.....11 00 00 (beta_P)
    BMC build date.......2023/02/04
    BMC last reset time..2023-03-22T08:20:04Z
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c
GetBmcInfo --file Supermicro_BMC.rom
```

Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.57 --ou
root --op 111111 -c GetBmcInfo --file Supermicro_BMC.rom
```

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

```
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/02) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.57:
================================================================================
Supermicro Update Manager (for UEFI BIOS) 2.10.0 (2022/11/02) (x86_64)
Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.
Managed system...........localhost
    BMC type.............X11_ATEN_AST2500_2
    BMC version..........12.63.00
    BMC ext. version......01 00 00
Local BMC image file......Supermicro_BMC.rom
    BMC type.............X11_ATEN_AST2500_2
    BMC version..........12.63.00
    FW image.............Signed
        Signed Key........NonRoT
================================================================================
Getting file 'remote_inband/2022-11-03_17-38-55_192.168.34.57/sum.log' from
'/root/sum_remote_inband/2022-11-03_17-37-49/sum.log' on 192.168.34.57.

End Remote In-Band execution on 192.168.34.57.
```

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, three-digit version numbers of BMC are supported.

5.4.2 Updating the BMC Firmware Image

Use the “UpdateBmc” command with BMC firmware image Supermicro_BMC.rom or bmc_image.tar for OpenBMC 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.
- The “UpdateBmc” command does not support AMI BMC FW. For OOB “UpdateBmc” usage, please use SUM version 1.4.2.
- The --overwrite_cfg option overwrites the current BMC configuration using the factory default values in the given BMC image file.
- The --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 details, 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.
- The option --skip_unknown is designed to skip all invalid tables and settings in the latest BMC configuration in the managed system.

OOB and In-Band 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]
```

Remote In-Band Syntax:

```
sum [-I Remote_INB | -I Remote_RHI -u <username> -p <password>] --oi <OS IP
address> --ou <OS username> [--op <OS password> | --os_key <OS private key> --
os_key_pw <OS private key password>] -c UpdateBmc --file <filename> [--
overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl] [--
remote_sum <remote sum path>]
```

Example:

OOB:

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

In-Band:

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

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

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
UpdateBmc --file Supermicro_BMC.rom
```

5.4.3 Getting BMC Settings

Use the “GetBmcCfg” command to execute SUM to get the current BMC settings from the managed system and save it in the BMCCfg.xml file or save it in the BMCCfg.bin file by “--dump” option.

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 getting 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.

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c GetBmcCfg --
file <BMCCfg.xml|BMCCfg.bin>  [--dump] [--overwrite]
```

Example:

OOB:

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

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

In-Band:

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

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

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
GetBmcCfg --file BMCCfg.xml --overwrite

[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
GetBmcCfg --file BMCCfg.bin --dump --overwrite
```

5.4.4 Updating BMC Settings

1. Follow the steps in *5.4.3 Getting 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.

Use the “ChangeBmcCfg” command with the updated BMCCfg.xml file to run SUM to update the BMC configuration or restore it with the BMCCfg.bin file by the "--restore" option.

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c ChangeBmcCfg
--file <BMCCfg.xml|BMCCfg.bin> [--restore]
```

Example:

OOB:

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

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

In-Band:

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

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

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
ChangeBmcCfg --file BMCCfg.xml

[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
ChangeBmcCfg --file BMCCfg.bin --restore
```

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

- The connection could be broken if the LAN configuration is changed.
- For in-band operation, all data of the <Configurations> element inside the <LAN> element is configurable.
- For OOB operation, if Redfish is not supported, all configurations inside the <LAN> element are read only.
- For OOB operation, the configurations of the <DynamicIPv6> element and the <StaticIPv6> element 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 “SetBmcPassword” command to execute SUM to update BMC user password.

OOB and In-Band 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>]]
```

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
SetBmcPassword [--user_id <user ID>] [[--new_password <new password> --
confirm_password <confirm password>] | [--pw_file <password file path>]] [--
remote_sum <remote sum 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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -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 Getting the BMC KCS Privilege Level

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

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key 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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -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 “SetKcsPriv” command 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 "LoadDefaultBmcCfg" command 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] [--clear_user_cfg [--load_unique_password | --
load_default_password]]
```

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
LoadDefaultBmcCfg [--preserve_user_cfg] [--clear_user_cfg [--
load_unique_password | --load_default_password]] [--remote_sum <remote sum
path>]
```

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]
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
LoadDefaultBmcCfg --preserve_user_cfg [--reboot]
```

Notes:

- The --load_unique_password option 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 "GetLockdownMode" command.

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
GetLockdownMode [--remote_sum <remote sum path>]
```

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
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -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 “SetLockdownMode” command 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 “BmcRotManage” command supports the following features on RoT systems of X12 and later platforms:

- **Getting Information on BMC**
  Use the “BmcRotManage” command with the option “--action GetInfo” to retrieve information on active BMC, backed-up BMC and Golden BMC.
- **Updating the Golden Image**
  Use the “BmcRotManage” command with the “--action UpdateGolden” option to replace the Golden image with an active BMC firmware.
- **Recovering BMC**
  Use the “BmcRotManage” command with the “--action Recover” option 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.
- **Downloading BMC Evidence:**
  Use the “BmcRotManage” command with the “--action DownloadEvidence” option to download BMC evidence.

Notes:

- BMC will be disconnected while updating the Golden image and recovering the firmware. Use the "GetMaintenEventLog" command to check the result afterwards. For details, see *5.5.3 Getting System Maintenance Event Log*.
- To execute the "Recover" and "DownloadEvidence" commands, the SFT-DCMS-SINGLE license is required.
- This command is only available for OOB and in-band usages restricted to the Redfish host interface.
- The "DownloadEvidence" action is only available after automatic or manual BMC recovery.
- The BMC evidence is a compressed gzip file.

OOB and In-Band Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
BmcRotManage --action <action> [--file <evidence.bin.gz>] [--overwrite]
```

Remote In-Band Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
BmcRotManage --action <action> [--file <evidence.bin.gz>] [--overwrite] [--
remote_sum <remote sum path>]
```

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
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c BmcRotManage --action
DownloadEvidence --file evidence.bin.gz
```

The console output contains the following information.

```
.....

Start generating BMC evidence.

....................Done

Start downloading BMC evidence............Done

BMC evidence file "evidence.bin.gz" is created.
```

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.
```

Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 --ou
root --op 111111 -c BmcRotManage --action UpdateGolden
```

5.4.13 Setting the BMC Reset Counter

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

OOB and In-Band Syntax:

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

Remote In-Band Syntax:

```
sum -I Remote_INB --oi <OS IP address> --ou <OS username> [--op <OS password> |
--os_key <OS private key> --os_key_pw <OS private key password>] -c
TimedBmcReset --delay  <BMC reset delay time> | --immediate
```

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.
```

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

The console output contains the following information.

```
The BMC will be reset immediately.
```

In-Band:

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

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -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.

5.4.14 Managing Remote Attestation

As a security mechanism, remote attestation provides a digital signature and allows users to manage measurement files on managed systems as well as local measurement files with confidence. A measurement file is a collection of states of the managed system, such as firmware version, firmware measurement, configuration data and hardware information. When a measurement file generated by managed system, a digital signature will be signed with the managed system's Device Attestation Key. Use the "Attestation" command to manage these files, six functions can be used with this command as follows:

- **Dumping Measurement Files**

  Use the "--action Dump" option to create and download a measurement file from the managed system, then save it as a local measurement file.

  - The --file option is optional for the Dump action. Without the --file option, the measurement file will be saved with the same file name as that on the managed system. In Windows OS, the character ':' will be replaced by '-' to save it in a valid filename.
  - The --nonce option is available with the Dump action. Without the --nonce input, SUM will use the current OS time of the manage system as the default nonce. When the managed system generates measurement files, the nonce will be written into the files. Thus, whenever a measurement file generates, the digital signature should not be reproduced if the managed system states was not changed.

- **Listing the Existing Measurement Files**

  Use the "--action List" option to list existing measurement files on the managed system.

- **Downloading Existing Measurement Files**

  Use the "--action Download" option to download an existing measurement file on the managed system.

  - Use the --file option to specify the measurement file on managed system.

- **Deleting Existing Measurement Files**

  Use the "--action Delete" option to delete an existing measurement file on the managed system.

  - Use the --file option to specify the measurement file on managed system.

- **Getting Information from Local Measurement Files**

  Use the “--action GetInfo” option to get information from local measurement files.

  - The GetInfo is only available for in-band usage and requires the --file and --file_only option.
  - Both --item and --showall options are only available for the GetInfo action and cannot be used at the same time.
  - The --root_cert option is only available for the GetInfo action.
  - The --extract_cert option is only available for the GetInfo action.

- **Comparing managed system or local measurement file with a referenced measurement file**

  Use the “--action Compare” option to compare managed system status or local measurement file with a referenced measurement file.

  - The action Compare requires --ref option, use the --ref option to specify the local referenced measurement file, the action Compare will dump a latest measurement from managed system and compare it with the local referenced measurement file.
  - Use the --file option to specify a local measurement file, the action Compare will compare the local measurement file with the local referenced measurement file, to check the local measurement and the referenced measurement are not both tampered, action Compare will still dump a latest measurement from managed system and check the certificate chain and signature states for the measurement files.
  - The --nonce option is also available with the Compare action; the nonce will be written into the latest measurement from managed system. Without the --nonce input, SUM will use the current OS time of the manage system as the default nonce.

OOB and In-Band Syntax:

```
sum [<-i <IP or host name> | -I Redfish_HI> -u <username> -p <password>] -c
Attestation --action <action> [--file <filename>] [--ref <filename>] [--
overwrite] [--item <item name>] [--showall] [--file_only] [--nonce <nonce>]
```

Remote In-Band Syntax:

```
sum -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS
username> [--op <OS password> | --os_key <OS private key> --os_key_pw <OS
private key password>] -c Attestation --action <action> [--file <filename>] [--
ref <filename>] [--overwrite] [--item <item name>] [--showall] [--file_only] [--
nonce <nonce>] [--remote_sum <remote sum path>]
```

Note: This command is only available for OOB and in-band usage restricted to the Redfish host interface when managing measurement files on the managed system.

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c Attestation --action
Dump --file measurement.bin --overwrite --nonce MY_NONCE_XXXX

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c Attestation --action
Dump

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

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c Attestation --action
Download --file measurement.bin

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c Attestation --action
Delete --file measurement.bin

[SUM_HOME]# ./sum -c Attestation --action GetInfo --file_only --file
measurement.bin
```

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
Attestation --action Download --file measurement.bin
```

Remote In-Band through Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 --ou
root --op 111111 -c Attestation --action Download --file measurement.bin
```

The console output contains the following information.

```
Measurement.............measurement.bin
    Nonce................2022-04-12T11:20:25+08:00
    Signature............Signed
    Certificate Chain....Verified
```

```
[SUM_HOME]# ./sum -c Attestation --action GetInfo --file_only --file
measurement.bin --extract_cert chain.pem
```

The console output contains the following information.

```
Measurement.............measurement.bin
    Nonce................2022-04-12T11:20:25+08:00
    Signature............Signed
    Certificate Chain....Verified
Device Identity Certificate PEM chain file "chain.pem" is created.
```

```
[SUM_HOME]# ./sum -c Attestation --action GetInfo --file_only --file
measurement.bin --item BMC_ACT_FW_VER
```

The console output contains the following information.

```
Measurement.............measurement.bin
    Nonce................2022-04-12T11:20:25+08:00
    Signature............Signed
    Certificate Chain....Verified

    Item: BMC_ACT_MEAS
    Description: BMC Firmware Measurement
    Value: A30CFFC59284658300654B8CDD5144B7C8CCDF3540B52EAF98FE0B7A3A8A4BB1E7FEA
2D89FC9F7BB701B35C1DDD53B43E08751F483573DB75E9F3D5653B0871A
```

```
[SUM_HOME]# ./sum -c Attestation --action GetInfo --file_only --file
measurement.bin --showall
```

The console output contains the following format information to shows all items in the measurement file.

```
    Item: <Item Name>
    Description: <Item Description>
    Value: <Item Value>
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c Attestation --action
Compare --ref reference_measurement.bin
```

The local measurement signature displays the following information:

Type	Description
Signed	The measurement file signature is signed by the Device Attestation Key and verified by the Device Attestation Public Key from the measurement file.
Verification failed	The measurement file signature cannot be verified by the Device Attestation Public Key from the measurement file.

The Certificate Chain of a local measurement file displays the following information:

Type	Description
Verified	The Device Identity Certificate Chain in a measurement file is verified back to the Root CA. The Device Attestation Certificate is verified by the Device Identity Certificate.
Verification failed	The Device Identity Certificate Chain in a measurement file cannot be verified back to the Root CA, or the Device Attestation Certificate cannot be verified by the Device Identity Certificate.

Root Certificates of local measurement files display the following information:

Type	Description
Matched	The Root CA Certificate matches with the input certificate file.
Mismatched	The Root CA Certificate does not match with the input certificate file.

5.4.15 Getting BMC LAN Settings

Use the “GetBmcLANCfg” command to execute SUM to get the current BMC LAN settings from the managed system and save them in the BMCLANCfg.xml file.hey

Notes:

- The 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 getting BMC LAN settings may be different. Be careful not to misuse them.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
GetBmcLANCfg --file <BMCLANCfg.xml> [--overwrite]
```

Example:

OOB:

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

In-Band:

```
[SUM_HOME]# ./sum -c GetBmcLANCfg --file BMCLANCfg.xml --overwrite

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetBmcLANCfg --file
BMCLANCfg.xml --overwrite
```

5.4.16 Updating BMC LAN Settings

1. Follow the steps in 5.4.15 Getting BMC LAN Settings.
2. Edit the configurable element values in the BMC LAN configuration text file BMCLANCfg.xml to the desired values described as those in 4.13 BMC LAN Configuration XML File Format.
3. Skip the unchanged tables in the text file by setting the Action attribute to "None." Note that this step is optional.
4. Remove unchanged tables/elements in the text file. Note that this step is optional.

Use the "ChangeBmcLANCfg" command with the updated BMCLANCfg.xml file to run SUM to update the BMC LAN configuration.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
ChangeBmcLANCfg --file <BMCLANCfg.xml>
```

Example:

OOB:

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

In-Band:

```
[SUM_HOME]# ./sum -c ChangeBmcLANCfg --file BMCLANCfg.xml

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c ChangeBmcLANCfg --file
BMCLANCfg.xml --overwrite
```

Note: Pay attention to the following when modifying content inside the XML element <LAN>:

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

5.4.17 Getting the BMC User List

Use the “GetBmcUserList” command to get the current BMC user list from the managed system.

Syntax:

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

Example:

OOB:

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

In-Band:

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

5.4.18 Setting the BMC User List

Use the “SetBmcUserList” command to set the current BMC user list from the managed system.

- **Add new BMC user**

  Use the “SetBmcUserList” command with the “--action Add” option to add a new BMC user.

- **Delete the BMC user**

  Use the “SetBmcUserList” command with the “--action Del” option to delete a BMC user.

- **Change BMC user privilege**

  Use the “SetBmcUserList” command with the “—action Level” option to change a BMC user privilege.

- **Change BMC user password**

  Use the “SetBmcUserList” command with the “--action SetPwd” option to change a BMC user password.

- Note: "No Access," a user privilege, is not supported after X11/H11 platforms.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c SetBmcUserList --
action <action> [--user_id <userid> --user_name <username> --user_password
<userpassword> --user_privilege <userprivilege>]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList --
action add --user_id 3 --user_name ADMIN123 --user_password ADMIn123 --
user_privilege 4
```

In-Band:

```
[SUM_HOME]# ./sum -c SetBmcUserList --action Del --user_id 3
```

5.4.19 Bootstrapping an Account for Redfish Host Interface

Use the BootStrappingAccount command to get a random account for Redfish Host Interface or delete an existing bootstapping account.

Notes:

- Administrator privileges are needed to delete a bootstrapping account.
- The function of deleting or checking an account is only available for using -I Redfish_HI. System reboot or BMC reset will automatically delete a bootstrapping account.
- Only local in-band usage is supported.
- Only two bootstrapping accounts are supported.
- To delete a bootstrapping account, the user name must be put into single quotation marks on Linux systems or double quotation marks on Windows systems.

Syntax:

```
sum [-I Redfish_HI -u <username> -p <password>] -c BootStrappingAccount --action
<action> [--user_name <username>]
```

```
Example:
```

In-Band:

```
[SUM_HOME]# ./sum -c BootStrappingAccount --action 1

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c BootStrappingAccount --
action 1

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c BootStrappingAccount --
action 3

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c BootStrappingAccount --
action 2 --user_name 'xxxxxxxxxxxxxxx'
```

5.4.20 Managing a RMCP Service Port

Use the “RmcpManage” command to get RMCP information and manage a RMCP service port.

Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
RmcpManage --action <GetInfo|Enable|Disable> [--port <port>]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c RmcpManage --action
GetInfo
The console output contains the following information.
Managed system................192.168.34.56
    RMCP Status...................Enable
    RMCP Port.....................623
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c RmcpManage --action
Enable --port RMCP:623
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c RmcpManage --action
Enable --port 623
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c RmcpManage --action Enable
--port RMCP:623
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p ADMIN -c RmcpManage --action Enable
--port 623
```

5.5 Event Log Management for a Single System

5.5.1 Getting System Event Log

Use the “GetEventLog” command 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] [--raw_data] [--no_banner]
```

Example:

OOB:

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

The console output contains the following information.

```
Event:1 Time:11/20/2022 16:58:35 Type:System

  Assertion: #0FF (System)| Event = Dedicated LAN Link Up



Event:2 Time:11/20/2022 16:58:45 Type:Power Supply

  Assertion: PS1 Status| Event = Presence detected



Event:3 Time:11/20/2022 16:58:46 Type:Voltage

  Assertion: CPU_VCCIN| Event = Lower Critical - going low

Reading = 0.89 V, Threshold = 1.20 V



Event:4 Time:11/20/2022 16:58:46 Type:Voltage
```

```
  Assertion: CPU_VCCIN| Event = Lower Non-recoverable - going low
Reading = 0.89 V, Threshold = 1.20 V


Event:5 Time:11/20/2022 17:01:33 Type:OS Boot
  Assertion: #000 (OS Boot)| Event = C: Boot completed
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetEventLog --
raw_data
```

The console output contains the following information.

```
SEL(   1) 01 00 02 BB 5C 7A 63 20 00 04 D0 FF 6F A3 01 FF

SEL(   2) 02 00 02 C5 5C 7A 63 20 00 04 08 C8 6F F0 FF FF

SEL(   3) 03 00 02 C6 5C 7A 63 20 00 04 02 13 01 52 34 47

SEL(   4) 04 00 02 C6 5C 7A 63 20 00 04 02 13 01 54 34 47

SEL(   5) 05 00 02 6D 5D 7A 63 41 00 04 1F 00 6F 01 FF FF
```

In-band:

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

[SUM HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetEventLog --raw_data -
-file EventLog.tx
```

5.5.2 Clearing the System Event Log

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

Notes:

- Both the BIOS and BMC event logs in BMC will be cleared immediately.
- The 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 [[--
current_password <current password>] | [--cur_pw_file <current password file
path>]] [--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 -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 --st and --et options are used to show logs at the specified time. With the “--count” option, the GetMaintenEventLog command can show the specified number of logs. With the “--file” option, 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 <MaintenEventLog.txt> [--overwrite]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetMaintenEventLog --st 20200601 --et 20200602 --count 5 --file MaintenEventLog.txt --overwrite
```

In-band:

```
[SUM_HOME]# ./sum -c GetMaintenEventLog --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 GetHostDump command with the “--action CreateDump” option to create the managed system’s crash dump file and download it from BMC.

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

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

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

  Use the GetHostDump command with the “--action DirectDump” option 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 “--file” option is required for both “--action CreateDump” and “--action DirectDump” options.
- The “--action CreateDump” option is not available on H12 RoT platforms.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -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
```

```
In-band:
```

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetHostDump --action 1 -
-file log.tgz
```

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 Getting CMM Firmware Image Information

Use the “GetCmmInfo” command to get 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
Supermicro_CMM.rom
```

The console output contains the following information.

```
Managed system...........192.168.34.56
    CMM type.............MicroCMM
    CMM version..........09.01
    ARM SUM version......1.0.0 (2021/12/10) (ARM)
Local CMM image file.....Supermicro_CMM.rom
    CMM type.............MicroCMM
    CMM version..........09.10
```

```
The following information is displayed only when the command "GetCmmInfo" is
executed with the option "--showall".

Blade ID: B6
==============
Node ID: 1
    Board model..........BH12SSi
    Status...............Normal
    BMC IP...............10.146.175.59
    BIOS version.........2.3a
    BIOS build date......2021/09/14
    BMC version..........75.00.06
    ARM SUM version......1.0.0 (2021/12/10) (ARM)
```

5.6.2 Updating the CMM Firmware Image

Use the "UpdateCmm" command with the CMM firmware image Supermicro_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 systems 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 three 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 three minutes and check the CMM web again.

- To update the "CSE-946ED-R2KJBOD" and "CSE-947HE2C-R2K05JBOD" JBOD systems, use the UpdateCmm command.

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
Supermicro_CMM.rom
```

5.6.3 Getting CMM Settings

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

Notes:

- Received tables/elements might not be identical between two managed systems. Only tables/elements supported for the managed system will be received.
- Configuration files in XML can be downloaded from CMM through the --download option. The feature is supported by 64MB CMM AST2400 only. For details, please refer to *5.14 Profile Update for a Single Blade System*.

Syntax:

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

Example:

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

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

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

5.6.4 Updating CMM Settings

1. Follow the steps in *5.6.3 Getting 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>
```

```
sum -i <IP or host name> -u <username> -p <password> -c ChangeCmmCfg {[--upload
--file <CmmCfg.xml>] | [--update Apply|Deploy]}
```

Example:

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

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

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

Notes:

- The connection might be lost if the LAN configuration is changed.
- The CMM configuration can be changed throuth the --upload option. Please use the GetCmmCfg command with option --download to obtain the CMM configuration file. The feature is supported by 64MB CMM AST2400 only.
- Please use the --skip_precheck option to upload and overwrite the existing CMM profile.
- The Update action “Apply” udpates CMM immediately with a CMM profile.
- For immediate update, if the scheduled update time in CMM profile expires, CMM configuration will be updated immediately.
- For scheduled updates, if the scheduled update time in CMM profile is in the future , CMM configuration will be updated at the scheduled update time.
- For details, please refer to *5.14 Profile Update for a Single Blade System*.
- The --skip_unknown option is designed to skip all invalid tables and settings in the latest CMM configuration in the managed system.

5.6.5 Setting Up a CMM User Password

Use the “SetCmmPassword” command 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 --user_id option, the user ID is set to 2 (as Administrator) by default.

5.6.6 Loading Factory CMM Settings

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

5.6.7 Getting BBP Firmware Image Information

Use the “GetBbpInfo” command to get 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 “UpdateBbp” command 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 that 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 --skip_check option 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 “GetBladePowerStatus” command 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 --blade option with index. To apply power action to a specified node of a blade system, you must assign a power action and the --blade and --node options 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 5 = softshutdown 24 = accycle
--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
```

5.6.11 Managing Profile Information

Use the “ProfileManage” command to manage the profile information on the managed system.

Option Commands	Descriptions

--action	Sets action to:
	Get = Get Profile List
	Edit = Edit Profile Info
	Delete = Delete Profile

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ProfileManage --action
<action> [--file <filename> [--overwrite]] [--file_id] [--profile_name] [--
profile_description] [--schedule_update_time][-showall]
```

Example:

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

The console output contains the following information.

```
Managed system...........192.168.34.56
Profile ID: 1

==============

Profile Type: Cmm

Profile Name: cmmcfg.xml

Profile Description: For_CMM

Schedule Update Time: 2021-09-07_14:28
```

```
Profile ID: 2

==============

Profile Type: System

Profile Name: systemcfg.xml

Profile Description: For_Blade_A1

Schedule Update Time: 2021-09-07_14:28
```

The following information is displayed only when the command “GetCmmInfo” is executed with the option “--showall”.

```
Managed system...........10.146.161.179


Profile ID: 1
==============
Profile Type: System
Profile Name: systemcfg_TEST.xml
Profile Description: TEST
Schedule Update Time: 2022-09-20_15:44
Profile Association:
    Blade:  B6 Node: 1 Status: Waiting for scheduling update
    Blade:  B6 Node: 2 Status: Waiting for receiving profile
    Blade:  B6 Node: 3 Status: Waiting for receiving profile
    Blade:  B6 Node: 4 Status: Waiting for receiving profile
    Blade: B10 Node: 1 Status: Waiting for scheduling update
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ProfileManage --
action Edit --file_id 2 --profile_description 'For_Blade_A2'
```

The console output contains the following information.

```
Profile ID "2" is edited.

Profile ID: 2

==============

Profile Type: System

Profile Name: systemcfg.xml

Profile Description: For_Blade_A2

Schedule Update Time: 2021-09-07_14:28
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ProfileManage --
action Delete --file_id 2
```

The console output contains the following information.

```
Profile ID "2" is deleted.
```

Notes:

- To download the current CMM configuration file or CMM profile, please use the GetCmmCfg command with the --download option. For details, please refer to *5.6.3 Getting CMM Settings*.
- To upload the CMM configuration file, please use the ChangeCmmCfg command with the --upload option. For details, please refer to *5.6.4 Updating CMM Settings (Single System)*.
- To update the CMM configuration, please use the ChangeCmmCfg command with the --update option. For details, please refer to *5.6.4 Updating CMM Settings (Single System)*.
- To download the current system configuration file or system profile, please use the GetSystemCfg command with the --download option. For details, please refer to *5.7.12 Getting System Settings*.
- To upload the system configuration file, please use the ChangeSystemCfg command with the --upload option. For details, please refer to *5.7.13 Updating System Settings*.

5.6.12 Receiving Switch Firmware Image Information

Use the “GetSwitchInfo” command to get the switch firmware image information as well as the local switch firmware image (with the --file option) from the managed system.

Syntax:

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

Notes:

- SBM-25G-P10 and BMB-25G-P10 are the same switch module.
- The --file option is used to parse SBM-25G-P10/BMB-25G-P10/MBM-XEM-002/MBM-GEM-004/SBM-25G-100 firmware image.

Example:

In-Band:

```
[SUM_HOME]# ./sum -c GetSwitchInfo --file Supermicro_Switch.bin --file_only
```

OOB:

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

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSwitchInfo --
dev_id A1,A2

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSwitchInfo --file
Supermicro_Switch.bin

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSwitchInfo --
dev_id A1,A2 --file Supermicro_Switch.bin
```

The console output contains the following information.

```
Local switch image file..Supermicro_Switch.bin
    Module name..........BMB-25G-P10
    Switch version.......1.0.0.21

Managed system...........192.168.34.56
[Switch A1]
==============
    Switch IP............192.168.34.100
    Switch type..........25G Pass-thru Module
    Module name..........SBM-25G-P10 (P1)
    Switch version.......1.0.0.21
    Power Status.........On
    Status...............Normal
[Switch A2]
==============
    Switch IP............192.168.34.101
    Switch type..........25G Pass-thru Module
    Module name..........SBM-25G-P10 (P1)
    Switch version.......1.0.0.8
    Power Status.........On
    Status...............Normal
[Switch B1]
==============
    Switch IP............192.168.34.102
    Switch type..........25G Pass-thru Module
    Module name..........SBM-25G-P10 (P1)
    Switch version.......1.0.0.21
    Power Status.........On
    Status...............Normal
[Switch B2]
==============
    Switch IP............192.168.34.103
    Switch type..........25G Pass-thru Module
    Module name..........SBM-25G-P10 (P1)
    Switch version.......1.0.0.21
```

```
Power Status.........On
Status...............Normal
```

5.6.13 Updating the Switch Firmware

Use the "UpdateSwitch" command with the switch firmware image Supermicro_Switch.bin to update the managed switch.

Notes:

- SBM-25G-P10 and BMB-25G-P10 are the same switch module.
- This command is only available for switch modules SBM-25G-P10/BMB-25G-P10/MBM-XEM-002/MBM-GEM-004/SBM-25G-100.
- The firmware version of switch module SBM-25G-100/BMB-25G-P10 must be equal to or greater than 1.0.0.10.
- The firmware version of switch module MBM-XEM-002 must be equal to or greater than 2.2.1.34.
- The firmware version of switch module MBM-GEM-004 must be equal to or greater than 1.3.0.8.
- The firmware version of switch module SBM-25G-100 must be equal to or greater than 1.4.0.11.
- The switch module must be rebooted to take effect.
- Without the --reboot option, the switch module will not restart after the UpdateSwitch command is executed. To reboot the switch module, execute the RebootSwitch command.
- To update switch firmware through CMM IP and switch device ID, you can use the --dev_id, --switch_user, and --switch_pw options.
- Please use the GetSwitchInfo command to get the switch device ID.

Syntax:

```
sum [-i <Switch IP or switch host name> -u <Switch username> -p <Switch
password>] -c UpdateSwitch --file <filename> [--reboot]
```

```
sum -i <CMM IP or CMM host name> -u <CMM username> -p <CMM password> -c
UpdateSwitch --file <filename> --dev_id <Switch device ID> --swtich_user <Switch
username> --switch_pw <Switch password> [--reboot]
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.100 -u ADMIN -p PASSWORD -c UpdateSwitch --file
Supermicro_Switch.bin --reboot
```

```
[SUM_HOME]# ./sum -i 192.168.34.100 -u ADMIN -p PASSWORD -c UpdateSwitch --file
Supermicro_Switch.bin --dev_id A1 --switch_user ADMIN --switch_pw ADMIN --reboot
```

5.6.14 Rebooting the Switch

Use the “RebootSwitch” command to reboot the managed switch.

Notes:

- SBM-25G-P10 and BMB-25G-P10 are the same switch module.
- This command is only available for the switch modules: SBM-25G-P10/BMB-25G-P10/MBM-XEM-002/MBM-GEM-004/SBM-25G-100.
- The firmware version of the switch module SBM-25G-100/BMB-25G-P10 must be equal to or greater than 1.0.0.10.
- The firmware version of the switch module MBM-XEM-002 must be equal to or greater than 2.2.1.34.
- The firmware version of the switch module MBM-GEM-004 must be equal to or greater than 1.3.0.8.
- The firmware version of the switch module SBM-25G-100 must be equal to or greater than 1.4.0.11.
- To reboot the managed switch through a CMM IP and a switch device ID, you can use the --dev_id, --switch_user, and --switch_pw options.
- Please use the GetSwitchInfo command to get the switch device ID.

Syntax:

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

```
sum -i <CMM IP or CMM host name> -u <CMM username> -p <CMM password> -c
RebootSwitch --dev_id <Switch Device ID> --swtich_user <Switch username> --
switch_pw <Switch password>
```

Example:

```
[SUM_HOME]# ./sum -i 192.168.34.100 -u ADMIN -p PASSWORD -c RebootSwitch
```

```
[SUM_HOME]# ./sum -i 192.168.34.100 -u ADMIN -p PASSWORD -c RebootSwitch --
dev_id A1 --switch_user ADMIN --switch_pw
```

5.7 Applications for a Single System

5.7.1 Sending an IPMI Raw Command

Use the “RawCommand” command 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.

5.7.2 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 Getting 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

5.7.3 Acquiring USB Port Access Mode (Inband Only)

Use the inband command “GetUsbAccessMode” command to get 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
```

5.7.4 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.

5.7.5 Controlling the UID of the Managed System

The UID is a unit identifier button for easy system location in large stack configurations. Use the "LocateServerUid" command 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
```

5.7.6 Booting into the ISO Image from HTTP Server

Use the “SetHttpBoot” command 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 [[--
current_password <current password>] | [--cur_pw_file <current password file
path>]] [--boot_lan <boot lan port>] [--boot_name <boot description>] --
image_url <URL> [--reboot] [--file <file name>]
```

```
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_name bootDescription --image_url http://192.168.12.78/iso/efishell.iso --
reboot
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetHttpBoot --
boot_lan 2 --boot_name bootDescription --file TLS.crt --image_url
https://[1234:ab5:0:c678:9012:345d:6e78:9f0a]/iso/efishell.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_name bootDescription --image_url
http://192.168.12.78/iso/efishell.iso --reboot
```

```
[SUM_HOME]# ./sum -c SetHttpBoot --boot_lan 2 --boot_name bootDescription --file
TLS.crt --image_url
https://[1234:ab5:0:c678:9012:345d:6e78:9f0a]/iso/efishell.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.
- Due to BIOS limitations, if an HTTP boot option exists in the BIOS configuration, please use the --boot_clean option to clean the HTTP boot option and then reset HTTP the boot option.
- When you execute the SetHttpBoot command on the FreeBSD 12 system, you may boot into FreeBSD instead of efishell.iso because of startup.nsh in the system. To prevent from it, you can delete startup.nsh or rename the startup.nsh file.

5.7.7 Managing KMS Server Configurations

Use the “KmsManage” command to change the KMS server configurations, upload TLS certificates and test the connection to the KMS server. The command only works on the X12/H12 and later platforms. Since SUM 2.9.0, users can save and configure the specific OEM functions for KMS features by using the [--file] option.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c KmsManage
[[--current_password <current password>] | [--cur_pw_file <current password
filename>]] [options…]
```

Option	Augment	Description
--server_ip	<server IP address>	Enters a KMS server IP address.
--second_server_ip	<second server IP>	Enters a second KMS server IP address.
--port	<port>	Enters an optional command port(s). The format of <port> is “TCP:5696” or “5696”. TCP is for KMS server port.
--time_out	<time out>	Enters a KMS server connection time-out.
--time_zone	<time zone>	Enters a correct time zone.
--client_username	<client username>	Enters a client identity: UserName.
--client_password	<client password>	Enters a client identity: Password.
--ca_cert	<CA certificate filename>	Uploads a CA certificate from the file.
--client_cert	<client certificate filename>	Uploads a client certificate from the file.
--pvt_key	<client private key>	Uploads a client private key from the file.
--pvt_key_pw	<private key password>	Uploads a client private key from the file.
--file	<file name>	When the “--action GetInfo” option is specified, save the OEM configurations to a file. Otherwise, update the OEM settings with the given configuration file.
--action	<action>	Sets the KMS management action to: 1 = GetInfo: Check the current KMS configurations. 2 = Probe: Test the connection to the specified KMS server. 3 = DeleteCA: Delete a CA certificate. 4 = DeleteCert: Delete a client certificate. 5 = DeletePvtKey: Delete a client private key.

Option	Augment	Description
		6 = DeleteAll: Delete all certificates and keys.
--reboot	N/A	Forces the managed system to reboot or power up after operation.
--post_complete	N/A	Wait for the managed system POST to complete after reboot.

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c KmsManage --server_ip
192.168.12.78 --port 5659 --ca_cert ca.crt --client_cert client.crt --pvt_key
private.key --action Probe --reboot
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c KmsManage --server_ip
192.168.12.78 --port TCP:5659 --ca_cert ca.crt --client_cert client.crt --
pvt_key private.key --action Probe --reboot
```

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

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

In-band:

```
[SUM_HOME]# ./sum -c KmsManage -server_ip 192.168.12.78 --port 5659 --ca_cert
ca.crt --client_cert client.crt --pvt_key private.key --action Probe --reboot
```

```
[SUM_HOME]# ./sum -c KmsManage --server_ip 192.168.12.78 --port TCP:5659 --
ca_cert ca.crt --client_cert client.crt --pvt_key private.key --action Probe --
reboot
```

```
[SUM_HOME]# ./sum -c KmsManage --action DeleteAll --reboot
```

```
[SUM_HOME]# ./sum -c KmsManage --action GetInfo
```

The console output contains the following information.

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


    KMS Server IP.................192.168.12.78

    Second KMS Server IP..........192.168.12.79

    KMS TCP Port Number...........5696

    KMS Time Out..................3

    KMS TimeZone..................GMT+0


    Client UserName...............user123

    Client Password...............******


    KMS TLS Certificate

    CA Certificate................Uploaded

    Client Certifcate.............Uploaded

    Client Private Key............Uploaded

    KMS Server Probe Status........KMS function works normally
```

Notes:

- To establish a TLS connection and enable the KMS service, it is required to provide the KMS server with the valid TLS certificates and private key. Please use the “--ca_cert”, “--client_cert” and “--pvt_key” options or use the “ChangeBiosCfg” command to upload the required files. For details, see *E.5.1 File Upload*.
- The “--action Probe” option is used to test the connection to the KMS server and requires a system reboot. Wait for the system POST to complete after reboot, and then use the “--action GetInfo” option to check the probe status. See the “KMS Server Probe Status” in the console output example above.

5.7.8 Getting System Settings

Use the "GetSystemCfg" command to execute SUM to get the current system settings from the managed system and save them in the SystemCfg.xml file. System settings include BIOS settings and BMC settings.

Notes:

- The tables/elements from the managed systems might not be identical. Only tables/elements supported by the managed systems will be acessed.
- A configuration file in XML can be downloaded from CMM through the --download option. The feature is only supported by 64MB CMM AST2400.
- For details on profile update, please refer to *5.14 Profile Update for a Single Blade System*.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c GetSystemCfg --file
<SystemCfg.xml> [--overwrite] [[--download] [--file_id]]
```

Example:

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

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSystemCfg --file
SystemCfg.xml --download --dev_id A1_1

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSystemCfg --file
SystemCfg_Cache.xml --download --file_id 2
```

5.7.9 Updating System Settings

1. Follow the steps in *5.7.12 Getting System Settings*.
2. Edit the configurable element values in the system configuration file SystemCfg.xml.See the steps in *5.3.4 Updating BIOS Settings Based on the Current BIOS Settings* and *5.4.4 Updating BMC Settings.*
3. Use the command ChangeSystemCfg with the updated SystemCfg.xml file to run SUM to update the system configuration.

Syntax:

```
sum [-i <BMC IP or host name> -u <username> -p <password>] -c ChangeSystemCfg --
file <SystemCfg.xml> [--reboot [--post_complete]]
```

```
sum -i <CMM IP or host name> -u <username> -p <password> -c ChangeSystemCfg {[--
update Apply|Deploy --dev_id <Device ID> --file_id <file ID> --reboot] | [--
upload --file SystemCfg.xml]}
```

Example:

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

```
[SUM_HOME]#./sum -i 192.168.34.56 -u ADMIN -p ADMIN -c ChangeSystemCfg --upload
--file SystemCfg.xml
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeSystemCfg --
update Apply --dev_id A1_1,B11_2,A10 --file_id 2 --reboot
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeSystemCfg --
update Apply --dev_id ALL --file_id 2 --reboot
```

Notes:

- The connection might be lost if the LAN configuration is changed.
- To update a profile, please refer to *5.6.11 Managing profile Information*.
- You can use the option --upload to change the CMM configuration. You can also use the GetCmmCfg command with the --download option to obtain the CMM configuration file. You should use the GetCmmCfg command with the --download option to get the uploaded file. The feature is supported by 64MB CMM AST2400 only.
- Please use the --skip_precheck option to upload and overwrite the existing system profile.
- The --reboot and --post_complete options are required for BMC OOB usage.
- Use the ProfileManage command to check the profile list before update.
- You can use the update action “Apply” to immedialy update the existing Blade systemwith the system profile.
- You can use the update action “Deploy” to update the existing and replaced Blade systems with the system profiles.

- For immediate update, if the scheduled update time in the system profile expires, the system configuration will be updated immediately.
- For scheduled update, if the scheduled update time in system profile is in the future, the system configuration will be updated at the scheduled update time.
- For details on profile update, please refer to *5.14 Profile Update for a Single Blade System*.
- The --skip_unknown option is used to skip all invalid menus, tables and settings in the latest system configuration in the managed system.

5.7.10 Invoking Redfish API

Use the “RedfishApi” command to invoke any Redfish API and display the response on screen.

Syntax:

```
sum [[-i <IP or host name>] | [-I Redfish_HI]] -u <username> -p <password> -c
RedfishApi --api <api path> [-v] [--request <http method>] [--file <file name>
[--overwrite]] [--data <request body>] [--retry <number>]
```

Option	Augment	Description
--api	<api path>	Redfish API path.
-v	N/A	Displays the response header.
--request	<http method>	The HTTP method should be one of the following: GET, POST, or PATCH. The default setting is GET.
--file	<file name>	Output the response to file instead of printing on screen.
--overwrite	N/A	Overwrite the output file.
--data	<request body>	The request body for the POST and PATCH methods. There are two usages: • Supplies the body in string directly. Note that the special character should be escaped. • Stores the body in a text file and supplies the file name. Note that you need to prepend an at character (@) to the file name, e.g., “--data @body.txt.”
--retry	<number>	Number of retry times. The default value is 3.

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c RedfishApi --api
/redfish/v1/TaskService

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c RedfishApi --request
PATCH --api /redfish/v1/TaskService --data "{\"ServiceEnabled\":true}"
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c RedfishApi  --request
PATCH --api /redfish/v1/TaskService -v --retry 1 --data @body.txt --file
response.txt --overwrite
```

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c RedfishApi --api
/redfish/v1/TaskService
```

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c RedfishApi --request
PATCH --api /redfish/v1/TaskService --data "{\"ServiceEnabled\":true}"
```

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c RedfishApi  --request
PATCH --api /redfish/v1/TaskService -v --retry 1 --data @body.txt --file
response.txt --overwrite
```

5.7.11 Remote Execution

Use the “RemoteExec” command to send files and execute shell commands on a remote system.

Syntax:

```
sum -I Remote_INB --oi <OS ip or host name> --ou <OS username> [--op <OS
password> | -os_key <OS private key> -os_key_pw <OS private key password>] -c
RemoteExec --remote_cmd <shell command> [--file <file name>]
```

Example:

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c
RemoteExec --remote_cmd "ls /tmp/ -l | grep test.sh" --file test.sh
```

```
[SUM_HOME]# ./sum -I Remote_INB --oi 192.168.34.57 --ou root --os_key privatekey
--os_key_pw privatekey_password -c RemoteExec --remote_cmd "ls /tmp/ -l | grep
test.sh" --file test.sh
```

Notes:

- The file will be copied to the path "/tmp/" in remote Linux systems.
- The stderr in the remote Linux system will be redirected to stdout.
- For use with approved third-party tools, please refer to *Appendix K. Using SUM to Run 3rd -Party Tools*.

5.8 Storage Management for a Single System

5.8.1 Getting RAID Firmware Image Information

Use the “GetRaidControllerInfo” command to get 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
```

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetRaidControllerInfo --
file RAID.rom --controller Broadcom --dev_id 0
```

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
```

In-band:

```
[SUM_HOME]# ./sum -c GetRaidControllerInfo --file RAID.rom --file_only
```

The console output contains the following information.

```
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 3108, 3808, 3816, 3908, 3916, 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:

- For X11 platforms, the “UpdateRaidController” command only supports Broadcom 3108.
- For X12 and later platforms, the “UpdateRaidController” command only supports Broadcom 3108, 3808, 3816, 3908, 3916, 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.

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 Getting RAID Settings

Use the “GetRaidCfg” command 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 Getting 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 "ChangeRaidCfg" command 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 “GetSataInfo” command 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 “GetNvmeInfo” command 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 192.168.3.4 -u ADMIN -p PASSWORD -c GetNvmeInfo --dev_id 0
```

The console output contains the following information.

```
NVMe Device information
======================
    [NVMe Controller(1)]
        Device ID: 0
        [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 “SecureEraseDisk” command 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	Serial Number	PSID	Password	New

Mode				Password
SAT3	9XF4AF7M	N/A	123456	111111
TCG	W472TJXH	HR1MJDCKLH4CD88ELEGDUE5J4UA3QGZZ	123456	111111

PSID.txt

```
W472TJXH;          HR1MJDCKLH4CD88ELEGDUE5J4UA3QGZZ
```

Password.txt

```
9XF4AF7M;          123456;    111111

W472TJXH;          123456;    111111
```

5.8.7.1 Execution Modes

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.

5.8.7.2 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.

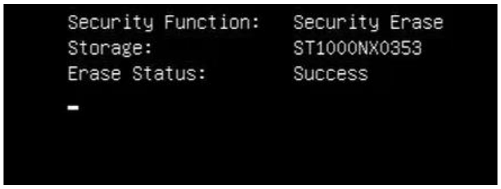
```
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file PSID.txt --
precheck
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file Password.txt --
precheck
Managed system............192.168.34.56
[HDD]
    Serial Number ..................9XF4AF7M
    Password Status ................NOT INSTALLED
    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.



```
Security Function:   Security Erase
Storage:             ST1000NX0353
Erase Status:        Success
-
```

After the task is complete, use the SUM GetCurrentBiosCfg command to check the result through BIOS configurations. Find the status code in the configuration file in xml format by “Last Status Code.” A status code of zero indicates the previous task was successful.

For details on the “GetCurrentBiosCfg” command, see *5.3.3 Getting Current BIOS Settings*.

5.8.7.3 Setting an 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.

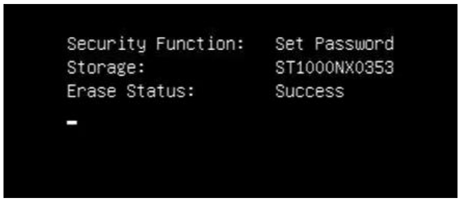
```
./sum -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file Password.txt --
precheck
Managed system............192.168.34.56
[HDD]
    Serial Number ..................9XF4AF7M
    Password Status ................NOT INSTALLED
    Security Mode ..................SAT3 Supported
    Applicable Action..............SetPassword
                      ..............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.



```
Security Function:   Set Password
Storage:             ST1000NX0353
Erase Status:        Success
-
```

4. After the task is complete, to check the execution result, run the SUM GetCurrentBiosCfg command (see *5.3.3 Getting 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 [[--current_password <current password>] | [--cur_pw_file <current password file path>]] --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 --action or --precheck options.
- 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 “SecureEraseRaidHdd” command 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 “GetRaidCfg” command 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) 2013-2022 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, .e.g., `--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) 2013-2022 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 “SecureEraseRaidHdd” command 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) 2013-2022 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) 2013-2022 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 ”GetPMemInfo” command to get the PMem firmware image information from the managed system as well as the local PMem firmware image (with the --file option).

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 the technical support of Supermicro.

5.8.10 Updating the PMem Firmware Image

Use the “UpdatePMem” command 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]] [[--current_password <current
password>] | [--cur_pw_file <current password file path>]] [--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.

5.8.11 Getting VROC Settings

Use the “GetVROCCfg” command to execute SUM to get the current VROC settings from the managed system and save it in the VROC.cfg.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.
- “NVME Mode Switch” in BIOS setting needs to set to “VMD” in order to use “GetVROCCfg” command.
- Host software in target system OS is required for VROC related commands.
- Target system needs to boot into OS in order to use VROC related commands.
- VROC related commands been tested on Red Hat Enterprise Linux 8.1.

Syntax:

```
sum [<-i <IP or host name> | -I <Redfish_HI>> -u <username> -p <password>] -c
GetVROCCfg [--file <VROC.cfg.xml> [--overwrite]]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetVROCCfg --file
VROC.cfg.xml --overwrite
```

In-band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetVROCCfg --file
VROC.cfg.xml --overwrite
```

5.8.12 Updating VROC Settings

1. Follow the steps in *5.8.11 Getting VROC Settings*.
2. Edit the configurable element values in the VROC configuration XML file VROC.cfg.xml as illustrated in *4.11 Format of the VROC Configuration XML File*.
3. Set the Action attribute as “None” to skip the unchanged tables in the XML file. Note that this step is optional.
4. Remove the unchanged tables/elements in the XML file. Note that this step is optional.
5. Use the “ChangeVROCCfg” command with the updated VROC.cfg.xml file to run SUM to update the VROC configuration.

Syntax:

```
sum [<-i <IP or host name> | -I <Redfish_HI>> -u <username> -p <password>] -c
ChangeVROCCfg --file <VROC.cfg.xml>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeVROCCfg --file
VROC.cfg.xml
```

In-band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c ChangeVROCCfg --file
VROC.cfg.xml
```

5.8.13 Control NVMe Device

Use the “ControlNvme” command to locate, insert or remove an NVMe device. You can use the GetNVMeInfo command to retrieve the required parameters, including device ID, group ID and slot number. Please see 5.8.6 Getting NVMe Informantion for details. This command supports four actions:

- **Locate:** locates the device by turning on its LED light.
- **StopLocate**: stops locating the device by turning off its LED light.
- **Insert**: inserts the device.
- **Remove**: removes the device.

Syntax:

```
sum [-i <IP or host name> -u <username> -p <password>] -c ControlNvme --action
<action> --dev_id <device ID> --group_id <group ID> --slot <slot number>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.3.4 -u ADMIN -p PASSWORD -c ControlNVMe --action
Locate --dev_id 0 --group_id 0 --slot 0
```

In-band:

```
[SUM_HOME]# ./sum -i 192.168.3.4 -c ControlNVMe --action Remove --dev_id 0 --
group_id 0 --slot 1
```

5.9 NIC Management for a Single System

5.9.1 Getting Add-On NIC Firmware Image Information

Use the “GetAocNICInfo” command to get the add-on NIC firmware information from the managed system as well as the add-on NIC local firmware image (with the --file option).

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -u
<username> -p <password>] -c GetAocNICInfo [--file <filename>] [--file_only] [--
dev_id <add-on NIC device ID >]
```

Example:

OOB:

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

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetAocNICInfo  --file
AOC_NIC.bin --dev_id 1,2,3
```

The console output contains the following information.

```
Add-on Network Interface Card Information
=========================================
Managed system........... 192.168.34.56
AOC NIC ID...............[1]
[General]
    AOC NIC Description..NIC device (riser:RSC-W2-66G4)
    AOC NIC Manufacturer.Supermicro
    AOC NIC Model........AOC-S100GC-i2C
    AOC NIC S/N..........WA214S004412
    AOC NIC Part Number..AOC-S100GC-i2C
    AOC NIC DeviceType...Simulated
    AOC NIC FW version...3.00 (N:06008A7A)
[PCIeInterface]
    PCIe Type............Gen4
    Maximum PCIe Type....Gen4
    Lanes In Use.........16
    Maximum Lanes........16

AOC NIC ID...............[2]
[General]
    AOC NIC Description..NIC device (riser:RSC-W2-66G4)
    AOC NIC Manufacturer.Supermicro
    AOC NIC Model........AOC-S100GC-i2C
    AOC NIC S/N..........WA20CS001831
    AOC NIC Part Number..AOC-S100GC-i2C
    AOC NIC DeviceType...Simulated
    AOC NIC FW version...3.00 (N:06008A7A)
[PCIeInterface]
    PCIe Type............Gen4
    Maximum PCIe Type....Gen4
    Lanes In Use.........16
    Maximum Lanes........16

AOC NIC ID...............[3]
[General]
    AOC NIC Description..NIC device (riser:RSC-WR-6)
    AOC NIC Manufacturer.Supermicro
    AOC NIC Model........AOC-STG-b2T
    AOC NIC S/N..........HA209S003222
    AOC NIC Part Number..AOC-STG-b2T
    AOC NIC DeviceType...Simulated
    AOC NIC FW version...20.8.157.0
[PCIeInterface]
    PCIe Type............Gen3
    Maximum PCIe Type....Gen4
    Lanes In Use.........8
    Maximum Lanes........8


Local AOC NIC image file.AOC_NIC.bin
    AOC NIC FW version...2.40 (N:04A075E6)
```

In-Band:

```
[SUM_HOME]# ./sum -c GetAocNICInfo  --file AOC_NIC.bin --file_only


Local AOC NIC image file.AOC_NIC.bin
    AOC NIC FW version...2.40 (N:04A075E6)
```

Note: This command is only available on X12/H12 and later platforms.

5.9.2 Updating the Add-On NIC Firmware Image

Use the “UpdateAocNIC” command with add-on NIC firmware image AOC_NIC.bin to update the managed system.

Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
UpdateAocNIC --file <filename> --dev_id <add-on NIC device ID> --reboot [--
post_complete]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateAocNIC --file
AOC_NIC.bin --dev_id 1 --reboot --post_complete
```

In-band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateAocNIC --file
AOC_NIC.bin --dev_id 1 --reboot
```

Notes:

- This command is only available on X12/H12 and later platforms.
- Use the “GetAocNICInfo” command to check the existing device IDs on the managed system.

5.10 PSU Management for a Single System

5.10.1 Getting PSU Information

Use the “GetPsuInfo” command 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
```

5.10.2 Updating the Signed PSU Firmware Image Requested by OEM

Use the “UpdatePsu” command 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
Supermicro_PSU.x0 --address 0x80
```

In-Band:

```
[SUM_HOME]# ./sum -c UpdatePsu --file Supermicro_PSU.x0 --address 0x80
```

Notes:

- During PSU firmware updating process, the updated PSU will be powered off. To use this command, the system needs to connect to at least two PSUs.
- Slave address of the PSU that needs to be updated can be found by executing the “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.

5.10.3 Getting Current Power Status of Managed System

Use the “GetPowerStatus” command 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
```

5.10.4 Setting Power Action of Managed System

Use the “SetPowerAction” command 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.

Proceeding to `power up the managed system.`

5.11 TPM Management for a Single System

Before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, the “TpmProvision” command 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 “GetTpmInfo” and “TpmManage” commands 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 Supermicro OTA. Depending on product design, either solution is implemented for the managed system. Supported OTA solution can be obtained on the output of the “GetTpmInfo” command. For more detailed information, please contact technical support.

The detailed information of TPM features is 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 (Supermicro OTA)	Yes	Yes	Required
GetTpmInfo (Intel OTA)	Yes	Yes	Required
TpmManage (Supermicro 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 (Supermicro OTA)	No	No	Yes
GetTpmInfo (Intel OTA)	No	No	Yes
TpmManage (Supermicro OTA)	No	No	Yes
TpmManage (Intel OTA)	No	No	Yes

5.11.1 Getting TPM Information

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the "GetTpmInfo" command to get 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 Supermicro 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 Supermicro 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 Supermicro 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 Supermicro 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 “Capability Flags”section is only for TPM 1.2.
- The --showall option is optional for the GetTpmInfo command.
- The “PS NV INDEX LCP Definition,” “AUX NV INDEX LCP Definition,” “PPI NV INDEX LCP Definition” and “Capability Flags” sections will be displayed when the option --showall is assigned.
- This command will query TPM module information through Intel OTA or Supermicro OTA.

5.11.2 Provisioning TPM Module

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, Use the "TpmManage" command 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 the 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 the --table_default option will execute TPM

provisioning with the default TPM provision table created by BIOS.

- Executing the TpmManage command with the --table option 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 “TpmManage” command with the “--clear_and_enable_dtpm” and “--reboot” options to enable TPM.
  b. Execute the “TpmManage” command with the “--provision” option to do TPM provision and then reboot the managed system manually.
  c. Execute the “TpmManage” command with the “--enable_txt_and_dtpm” and “--reboot” options to enable TPM and TXT.

On platforms before X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, use the “TpmProvision” command 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).

5.11.3 Enabling and Clearing TPM Module Capabilities

On platforms after X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets, use the "TpmManage" command 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 “--clear_and_enable_dtpm_txt” and “--enable_txt_and_dtpm” options cannot be used when TPM is not provisioned.
- The “--disable_dtpm” option cannot be used when TXT is enabled.
- Please execute the “GetTpmInfo” command to obtain the OTA supported type before using TPM.
- 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 "TpmProvision" command with the "--cleartpm" and "--reboot" options 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.

5.12 GPU Management for a Single System

5.12.1 Getting GPU Information

Use the “GetGpuInfo” command to get the current NVIDIA GPU information from the managed system.

Syntax:

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

Example:

OOB:

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

In-Band:

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

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -c GetGpuInfo
```

- The console output contains the following information of the managed system with add-on GPU cards installed.
  - X11/H11 and earlier platforms

```
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
```

- X12/H12 and later platforms

```
GPU information

===================

[GPU(1)]

    Brand                          : NVIDIA

    Location                       : 2

    Model                          : Tesla P100-PCIE-12GB

    Serial Number                  : 0325117155632

    Part Number                    : 15F7-893-A1
    Firmware Version            : 86.00.4D.00.03
    GPU GUID                    : df5f42692dc92dc40e301b746505f5ae
    Board Part Number           : 900-2H400-0010-000
    InfoROM Version             : H400.0202.00.01
    Memory Vendor               : S
    Temperature(C)              : 1 degreeC
```

- The console output contains the following information for HGX2 system on X11/H11 systems.

```
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
```

- The console output contains the following information for HGX system on X12/H12 systems.

```
HGX information

===================

CEC Version....................3.9
```

```
FPGA Version...................2.A5

[GPU(1)]

    Brand                      : NVIDIA

    Location                   : 0

    Model                      : NVIDIA A100-SXM4-80GB

    Part Number                : 20B2-895-A1

    Firmware Version           : 92.00.45.00.05

    GPU GUID                   : 74f76243ff58e56784bed8928ff4ff71

    InfoROM Version            : G506.0210.00.03

    Temperature(C)             : 32 degreeC


[GPU(2)]

    Brand                      : NVIDIA

    Location                   : 0

    Model                      : NVIDIA A100-SXM4-80GB

    Part Number                : 20B2-895-A1

    Firmware Version           : 92.00.45.00.05

    GPU GUID                   : fbec45bdd281d823c9b30edf38379387

    InfoROM Version            : G506.0210.00.03

    Temperature(C)             : 29 degreeC
```

```
[GPU(3)]
    Brand                      : NVIDIA
    Location                   : 0
    Model                      : NVIDIA A100-SXM4-80GB
    Part Number                : 20B2-895-A1
    Firmware Version           : 92.00.45.00.05
    GPU GUID                   : e34eb0db342be31e5e15855f2e91a00b
    InfoROM Version            : G506.0210.00.03
    Temperature(C)             : 30 degreeC

[GPU(4)]
    Brand                      : NVIDIA
    Location                   : 0
    Model                      : NVIDIA A100-SXM4-80GB
    Part Number                : 20B2-895-A1
    Firmware Version           : 92.00.45.00.05
    GPU GUID                   : 06f4a98a2223e016230a396678a546c1
    InfoROM Version            : G506.0210.00.03
    Temperature(C)             : 32 degreeC

[GPU(5)]
```

```
    Brand                       : NVIDIA
    Location                    : 0
    Model                       : NVIDIA A100-SXM4-80GB
    Part Number                 : 20B2-895-A1
    Firmware Version            : 92.00.45.00.05
    GPU GUID                    : 37ed231dc89f1f68194c3b9b4ed2f78b
    InfoROM Version             : G506.0210.00.03
    Temperature(C)              : 33 degreeC


[GPU(6)]
    Brand                       : NVIDIA
    Location                    : 0
    Model                       : NVIDIA A100-SXM4-80GB
    Part Number                 : 20B2-895-A1
    Firmware Version            : 92.00.45.00.05
    GPU GUID                    : 4f64a3e7fc36c95cf0b1e2811571fa8e
    InfoROM Version             : G506.0210.00.03
    Temperature(C)              : 29 degreeC


[GPU(7)]
    Brand                       : NVIDIA
    Location                   : 0
    Model                      : NVIDIA A100-SXM4-80GB
    Part Number                : 20B2-895-A1
    Firmware Version           : 92.00.45.00.05
    GPU GUID                   : 4afc961d2be7063faff75e72fe828c04
    InfoROM Version            : G506.0210.00.03
    Temperature(C)             : 29 degreeC


[GPU(8)]
    Brand                      : NVIDIA
    Location                   : 0
    Model                      : NVIDIA A100-SXM4-80GB
    Part Number                : 20B2-895-A1
    Firmware Version           : 92.00.45.00.05
    GPU GUID                   : fd2a3f33649568183bb50a08fec1b5b4
    InfoROM Version            : G506.0210.00.03
    Temperature(C)             : 32 degreeC


[HGX Delta System Temperature]
[HBM]
    Reading Temperature        : 36 degreeC
    HBM  1 Temperature         : 36 degreeC

    HBM  2 Temperature         : 33 degreeC

    HBM  3 Temperature         : 33 degreeC

    HBM  4 Temperature         : 35 degreeC

    HBM  5 Temperature         : 35 degreeC

    HBM  6 Temperature         : 33 degreeC

    HBM  7 Temperature         : 33 degreeC

    HBM  8 Temperature         : 36 degreeC

[NVLink Switch]

    Reading Temperature        : 31 degreeC

    NVLink SW  1 Temperature   : 30 degreeC

    NVLink SW  2 Temperature   : 29 degreeC

    NVLink SW  3 Temperature   : 31 degreeC

    NVLink SW  4 Temperature   : 31 degreeC

    NVLink SW  5 Temperature   : 31 degreeC

    NVLink SW  6 Temperature   : 30 degreeC

[PCI Switch]

    Reading Temperature        : 57 degreeC

    PCI SW  1 Temperature      : 24 degreeC

    PCI SW  2 Temperature      : 57 degreeC

    PCI SW  3 Temperature      : 57 degreeC
    PCI SW  4 Temperature      : 55 degreeC

    PCI SW  5 Temperature      : 56 degreeC

[GPU Board]

    Reading Temperature        : 36 degreeC

    GPU Board  1 Temperature   : 36 degreeC

    GPU Board  2 Temperature   : 26 degreeC

[PLX]

    Reading Temperature        : 68 degreeC

    PLX 1 Temperature          : 63 degreeC

    PLX 2 Temperature          : 68 degreeC

    PLX 3 Temperature          : 68 degreeC

    PLX 4 Temperature          : 64 degreeC

[Pump]

    Pump Temperature           : 0 degreeC
```

Note: For more details on support, please refer to the following links.

○ Supermicro - Qualified Platform List for NVIDIA vGPU

○ Supported GPU System Model

5.12.2 Updating the GPU Firmware Image

Use the “UpdateGpu” command with the CEC/FPGA of GPU firmware image to update the GPU firmware of a managed system by SUM.

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
UpdateGpu --item <CEC|FPGA> --file <filename>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateGpu --file
GPU_CEC.bin --item CEC
```

The console output contains the following information.

```
Supermicro Update Manager (for UEFI BIOS) 2.9.0 (2022/03/07)(x86_64)

Copyright(C) 2013-2022 Super Micro Computer, Inc. All rights reserved.

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

     HGX Model................HGX A100

   CEC version................4.0

  FPGA version................3.03

Local GPU CEC image file......GPU_CEC.bin

Status: Start updating CEC for 192.168.34.56

************************************WARNING****************************

    Do not remove AC power from the server.

************************************************************************
```

```
Uploading GPU CEC FW...Done

Updating GPU CEC
FW ...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done

Status: GPU CEC is updated for 192.168.34.56

Note: You have to reboot or power up the system for the changes to take
effect
```

In-band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateGpuFw --file
GPU_FPGA.bin --item FPGA
```

Note: This command is only available on X12/H12 and later platforms. It is only used for updating NVIDIA HGX A100 8-GPU system firmware.

5.13 CPLD Management for a Single System

5.13.1 Getting CPLD Firmware Image Information

Use the “GetCpldInfo” command to get the CPLD firmware image information from the managed system as well as the local CPLD firmware image (with the --file option).

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c
GetCpldInfo [--file <filename> [--file_only] [--extract_measurement]
```

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...........192.168.34.56
    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
```

```
[SUM_HOME]# ./sum -c GetCpldInfo -I Redfish_HI -u ADMIN -p ADMIN --file CPLD.bin
--extract_measurement
```

The console output contains the following information.

```
Managed system...........192.168.34.56
    CPLD version.........F0.09.46
    CPLD signed..........Signed

Local CPLD image file....CPLD.bin
    CPLD version.........F0.0D.5A
    FW image.............Signed
        Signed Key.......RoT
        Measurement......7F3095B7E9ABC6F982719F7A293C68A02373C2BF5C6B7C160D5E980
D90E79708932E6F577B74814C244B81D76F2925F1F456E734CFE67AA8E9CA57C4DA894757
```

A 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.

5.13.2 Updating the CPLD Firmware Image

Use the “UpdateCpld” command with the 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.
- The system needs to be powered off while updating the CPLD firmware.

5.14 AIP Management of a Single System

5.14.1 Getting AIP CPLD Information

Use the “GetAipCpldInfo” command to get the current AIP (AI Processor) CPLD information from the managed system installed with AIP.

Syntax:

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

Example:

OOB:

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

The console output contains the following information.

```
AIP CPLD information

====================

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

    [AIP Device 1]

        AIP Model.......................Habana Gaudi HL205

        AIP CPLD version................1A

    [AIP Device 2]

        AIP Model.......................Habana Gaudi HL205

        AIP CPLD version................1A

    [AIP Device 3]

        AIP Model.......................Habana Gaudi HL205
        AIP CPLD version................1A

    [AIP Device 4]

        AIP Model.......................Habana Gaudi HL205

        AIP CPLD version................1A

    [AIP Device 5]

        AIP Model.......................Habana Gaudi HL205

        AIP CPLD version................1A

    [AIP Device 6]

        AIP Model.......................Habana Gaudi HL205

        AIP CPLD version................1A

    [AIP Device 7]

        AIP Model.......................Habana Gaudi HL205

        AIP CPLD version................1A

    [AIP Device 8]

        AIP Model.......................Habana Gaudi HL205

        AIP CPLD version................1A
```

Note: This command is now only available on the SYS-420GH-TNGR system.

5.14.2 Updating the AIP CPLD Firmware Image

Use the “UpdateAipCpld” command with the given AIP (AI Processor) CPLD firmware image to run SUM to update the AIP CPLD firmware of managed systems installed with AIP.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c UpdateAipCpld --file
<filename>
```

Example:

OOB:

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

The console output contains the following information.

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

    AIP FW version.................1A;1A;1A;1A;1A;1A;1A;1A

Local AIP image file...............AIP_CPLD.bin

Status: Start updating AIP CPLD for 192.168.34.56

************************************WARNING*************************************

    Do not remove AC power from the server.


Uploading FW.......Done

Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done

Status: AIP CPLD is updated for 192.168.34.56

Update Complete, Please wait for BMC reboot, about 5 mins.
```

```
..................................................

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

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

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

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

.............................................Done
```

Note: This command only supports the SYS-420GH-TNGR system.

5.16 Profile Update for a Single Blade System

Profile update is used to manage CMM and system configurations for the Blade system and update configuration at scheduled times. Profile update is only supported on the Blade system with 64MB CMM AST2400. You can use the ChangeCmmCfg/ChangeSystemCfg command and the --upload option to upload one CMM profile, up to twenty system profiles, and CMM/Blade system configurations to CMM.

Use the ProfileManage command to edit and get the existing profile information from CMM. Note that there is a space limit on Profiles. Once the space is full, use the ProfileManage command to delete unnecessary profiles and upload new profiles. Each profile name on CMM is unique. Different profiles with the same profile names cannot exist on CMM at the same time.

Commands	Descriptions
ProfileManage	• Gets and edits profile information or deletes the profile on CMM. • Provides profile association information between specified profile and the selected Blade systems.
GetCmmCfg	Downloads the current or repository CMM configuration from CMM.
ChangeCmmCfg	• Uploads the CMM configuration to CMM. • Updates the CMM configuration to CMM by the existing CMM configuration on CMM.
GetSystemCfg	Downloads the current or repository system configuration from CMM.
ChangeSystemCfg	• Uploads the system configuration to CMM. • Updates the system configuration to a Blade system through CMM with the existing system configuration on CMM.

5.16.1 Profile Update Rule

SUM supports two update actions, apply and deploy. The update actions should be paired with the scheduled update time in the profile to update the managed system.

The update the “Apply”action can be used to update the existing Blade systems at either scheduled time or immediately. You can also use the update the “Deploy” action to update the Blade systems that have been existing or replaced. If the Blade system is busy, BMC will update the system configuration after the ongoing task is complete. By default, the file creation time will be treated as the default value in “ScheduledUpdateTime,” and the file can be used for immediate update.

One Blade system only accepts one single update rule. The new rule always replaces the older rule.

Update Action	Scheduled Time	Operation
Apply	Past time	Updates the Blade system immediately.
Apply	Future time	Updates the Blade system at scheduled time.
Deploy	Past time	Immediately updates the Blade systems that have been existing or replaced.
Deploy	Future time	Updates the Blade systems that have been existing or replaced at scheduled time.

For immediate update:

- Updates the existing Blade systems immediately.
- If the system is busy, it will update the configuration after the ongoing task is complete.
- If the the Blade system is either replaced or re-plugged, CMM will send the configuration to the new Blade after the HW change, and then update the Blade configuration.

For schedule update:

- Updates the existing Blade systems at scheduled time.
- If the system is busy at scheduled time, the configuration will be updated after the ongoing task is complete.
- If the Blade system is replaced or re-pluggd after the scheduled updatetime, CMM will send the configuration to the new Blade after hardware change, and then update the Blade configuration.

5.16.2 Profile Management

Follow the steps below to edit a profile on CMM.

1. Execute the ProfileManage command with the --Action Get option to get the existing profile list on CMM. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.
2. Check profile information on the list.
3. Execute the ProfileManage command with the --Action Edit, --file_id and [--profile_name/ --profile_description/ --schedule_update_time] options to edit existing profile information on CMM. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.
4. Execute ProfileManage command with the --Action Get option again to check whether the profile information is changed. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.

5.16.3 Updating CMM Configurations

Follow the steps below to update the CMM configuration.

1. Execute the ProfileManage command with the --Action Get option to get the existing profile list on CMM to check if any profile is available for update. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.
2. Execute the GetCmmCfg command with the --Download option to download the current CMM configuration file for profile update. For more details, please refer to *5.6.3 Getting CMM Settings (Single System)*.
3. Edit the CMM configuration file to set the unique profile name, edit profile description and schedule update time.
4. Execute the ChangeCmmCfg command with the --Upload option to upload the local CMM configuration file to CMM. For more details, please refer to *5.6.4 Updating CMM Settings (Single System)*.

5. Execute the ProfileManage command with the --Action Get option to get the existing profile list on CMM, then check if the profile is uploaded successfully before update. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.

6. Execute the ChangeCmmCfg command with the --Update option to update the selected CMM configuration the profile. For more details, please refer to *5.6.4 Updating CMM Settings (Single System)*.

7. Execute the ProfileManage command with the --Action Get, --file_id <profile ID> and --showall options to check whether the task is executed. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.

Note: Use the ProfileManage command to upload the profile information to CMM, which can be updated. Please refer to *5.6.7 Managing profile Information (Single System)*.

5.16.4 Updating Blade Configurations

Follow the steps below to update the Blade system configuration.

1. Execute the ProfileManage command with the --Action Get option to get the existing profile list on CMM to check if any profile is available for update. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.

2. Execute the GetSystemCfg command with the --Download option to download the current system configuration file.

3. Edit the system configuration file to set a unique profile name, profile description, and scheduled update time.

4. Execute the ChangeSystemCfg command with the --Upload option to upload the local system configuration file to CMM. For more details, please refer to *5.7.12 Getting System Settings*.

5. Execute the ProfileManage command with the --Action Get option to get the existing profile list on CMM to check if the profile is uploaded successfully before update. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.

6. Execute the ChangeSystemCfg command with the --Update and --dev_id options to update the system configuration to the Blade system through CMM by the selected profile. For more details, please refer to *5.7.13 Updating System Settings*.

7. Execute the ProfileManage command with the --Action Get, --file_id <profile ID> and --showall options to check whether the task is executed. For more details, please refer to *5.6.11 Managing profile Information (Single System)*.

Note: Use the ProfileManage command to upload the profile information to CMM, which can be updated later. Please refer to *5.6.7 Managing profile Information (Single System)*.

5.17 TwinPro Management for a Single System

5.17.1 Getting TwinPro Settings

Use the “GetTpCfg” command to execute SUM to get the current TwinPro settings from the managed system and save it in the TpCfg.xml file.

OOB and In-Band Syntax:

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

Example:

OOB:

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

In-Band:

```
[SUM_HOME]# ./sum -c GetTpCfg --file TpCfg.xml --overwrite
```

5.17.2 Updating TwinPro Settings

1. Follow the steps in *5.16.1 Getting TwinPro settings*.
2. Edit the configurable element values in the BMC configuration text file TpCfg.xml to the desired values as illustrated in *4.9 Format of TwinPro 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.

Use the “ChangeTpCfg” command with the updated TpCfg.xml file to run SUM to update the BMC configuration.

OOB and In-Band Syntax:

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

Example:

OOB:

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

In-Band:

```
[SUM_HOME]# ./sum -c ChangeTpCfg --file TpCfg.xml
```

5.18 CDU Management for a Single System

5.18.1 Getting CDU Information

Use the “MonitorCDUStatus” command to execute SUM to show the current CDU Web UI Status remotely. With the --file option, the CDU status can be saved into an output file.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c MonitorCDUStatus --
action GetStatus|1 [--file <CDUStatus.txt>] [--overwrite]
```

Example:

OOB:

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

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MonitorCDUStatus --
action GetStatus --file CDUStatus.txt --overwrite
```

The console output contains the following information.

```
CDU (Coolant Distribution Unit) System Status

[System Status]

      CDU Status: OK

      Emergency Status: OK

      Operation Mode: auto

[Device Status]

  Device Name                     Status     Value       Operation Time(h:m)

  --------------                  -------    -------     -------------------
```

```
   Power Top                         OK
   Power Bottom                      OK
   Pump Left                         OK         6281[RPM]          108:34
   Pump Right                        OK         6281[RPM]          108:34
   Valve Left                        OK         100[%]
   Valve Right                       OK         100[%]
   CDU Status                        OK
   Sensor Module                     OK
   Leak Detection                    OK
   Humidity Sensor                   OK
   Liquid Level                      Low
   Leak (External Ch1)               N/A
   Leak (External Ch2)               N/A
   Liquid Level (External Ch1)       N/A
   Liquid Level (External Ch2)       N/A
[Sensor Value]
   Sensor Name                       Status                        Value
   --------------                    -------                       -------
   Temperature from Server            Warning level                25.52[°C]
   Temperature to Server              Valid                        42.15[°C]
   Temperature from Facility          Valid                        23.20[°C]
   Temperature to Facility            Valid                           23.12[°C]

   Temperature ambient                                                20.69[°C]

   Pressure Server                    Warning level                   0.230[MPa]

   Pressure Facility                  Alert level                     0.000[Ma]

   Flow Rate Server                   Alert level                     0.00[L/min]

   Flow Rate Facility                 Alert level                     0.00[L/min]

   Humidity                                                           66.20[%RH]

   Dew Point                          OK                              14.16[°C]

   Heat Load                                                          -0.00[kW]
```

5.18.2 Setting CDU Alert Setting

Use the “MonitorCDUStatus” command to execute SUM to set CDU alert setting with the CDU_alert_setting.json file.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c MonitorCDUStatus --
action SetCfg|2 --file < CDU_alert_setting.json file>
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c MonitorCDUStatus --
action SetCfg --file CDU_alert_setting.json
```

5.18.2.1 MonitorCDUStatus JSON File Format

A CDU alert setting JSON file format is explained below. The sample file is named as "CDU_alertsetting_sample.json" and bundled in the SUM release package.

The table lists the names on the CDU Web UI and in the JSON file.

- Device Status Table

CDU Web UI	CDU sample.json	CDU Web UI	CDU sample.json
Leak Detection	leak	Sensor Module	sensor
Power Top	power1	Humidity Sensor	humidity
Power Button	power2	Liquid Level (OK)	level_upper
Control Unit	cunit	Liquid Level (Low)	level_lower
Pump Left	pump1	Liquid Leak (External Ch1)	leak_ext_ch1
Pump Right	pump2	Liquid Leak (External Ch2)	leak_ext_ch2
Valve Left	valv1	Liquid Level (External Ch1)	level_ext_ch1
Valve Right	valv2	Liquid Level (External Ch2)	level_ext_ch2

- Sensor value table

CDU Web UI	CDU sample.json	CDU Web UI	CDU sample.json
Temperature (From Server)	temp_from_server	Pressure (Server)	press_server
Temperature (To Server)	temp_to_server	Pressure (Facility)	press_facility
Temperature (From Facility)	temp_from_facility	Flow Rate (Server)	flow_server
Temperature (To Facility)	temp_to_facility	Flow Rate (Facility)	flow_facility

You can decide whether to trap the items under "trap" in each device. The allowable value is "true" or "false." Regardless of the "trap" status of items, it will affect the CDU status.

You can set the maximum and minimum values of alerts and warnings for Temperature, Pressure, and Flow Rate to monitor the CDU sensors status.

For each alert and waring level min. and max. thresholds of sensors, please refer to the following table.

CDU sample.json	Level	Maximum	Minimum
temp_from_server(°C)	Alert	80	0
	Warning	80	0
temp_to_server(°C)	Alert	80	0
	Warning	80	0
temp_from_facility(°C)	Alert	80	-10
	Warning	80	-10
temp_to_facility(°C)	Alert	80	0
	Warning	80	0
press_server(MPa)	Alert	1	0
	Warning	1	0
press_facility(MPa)	Alert	1	0
	Warning	1	0
flow_server(L/min)	Alert	150	0
	Warning	150	0
flow_facility(L/min)	Alert	150	0
	Warning	150	0

5.19 Backplane Management for a Single System

5.19.1 Getting Multi-Node EC Firmware Image Information

Use the “GetMultinodeEcInfo” command to get the multi-node EC firmware image information from the managed system as well as the local multi-node EC firmware image (with the --file option).

Syntax:

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

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.184.11.65 -u ADMIN -p PASSWORD -c GetMultinodeEcInfo
```

The console output contains the following information.

```
Managed system............192.184.11.65
    EC ID.................A7
    EC version............1.20
```

In-Band:

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

The console output contains the following information.

```
Managed system............169.254.3.254
    EC ID.................A7
    EC version............1.20
```

```
[SUM_HOME]# ./sum -c GetMultinodeEcInfo --file EC.bin --file_only
```

The console output contains the following information.

```
Local EC image file.......EC.bin

    EC ID.................A7

    EC version............1.20
```

5.19.2 Updating the Multi-node EC Firmware Image

Use the “UpdateMultinodeEc” command with the given multi-node EC firmware image EC.bin to run SUM to update the multi-node EC firmware of a managed system.

Syntax:

```
sum <-i <IP or host name> | -I Redfish_HI> -u <username> -p <password> -c
UpdateMultinodeEc --file <filename>
```

Example:

OOB:

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

In-Band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateMultinodeEc --file
EC.bin
```

The console output contains the following information.

```
Managed system.....................169.254.3.254

    EC ID..........................A7

    EC version.....................1.20
```

```
Local EC image file................EC.bin

    EC ID..........................A7

    EC Version.....................1.20

Status: Start updating Multi-node EC for 169.254.3.254

************************************WARNING*************************************

    Do not remove AC power from the server.

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

Uploading FW...Done

Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done

Status: Multi-node EC is updated for 169.254.3.254
```

- **Note:** This command can be only run on a system on node A to update EC FW for multi nodes.

5.19.3 Getting Backplane CPLD Firmware Information

Use the “GetBackplaneCpldInfo” command to get the backplane CPLD firmware information from the backplane on managed system.

Syntax:

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

Example:

OOB:

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

The console output contains the following information.

```
Backplane CPLD information
==========================
Managed system..........................192.168.34.56
    [Backplane 0]
        Backplane Model.................BPN-NVMe4-217BHQ-S6
        Backplane CPLD ID...............0023
        Backplane CPLD Revision.........0C
```

In-Band:

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

The console output contains the following information.

```
Backplane CPLD information
==========================
Managed system..........................localhost
    [Backplane 0]
        Backplane Model.................BPN-NVMe4-217BHQ-S6
        Backplane CPLD ID...............0023
        Backplane CPLD Revision.........0C
```

Notes:

- This command is only available on X10/H10 and later platforms with storage backplanes installed.
- A maximum of four backplane CPLDs can be detected.

5.19.4 Updating the Backplane CPLD Firmware Image

Use the “UpdateBackplaneCpld” command with the backplane CPLD firmware image to update the backplane CPLD firmware of a managed system by SUM.

Syntax:

```
sum -i <IP or host name> -u <username> -p <password> -c UpdateBackplaneCpld <--
index <0|1|2|3> --file BPN_CPLD.jed | --update_list
0:BPN_CPLD.jed[,1:Backplane_CPLD.jed]...]> --manual_ejected
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBackplaneCpld -
-index 0 --file BPN_CPLD.jed --manual_ejected
```

The console output contains the following information.

```
Status: Start updating Backplane CPLD for 192.168.34.56

************************************WARNING****************************

    Do not remove AC power from the server.

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

Warning: All drives on backplane will be force ejected due to backplane
reset after update.
```

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

     Backplane CPLD ID...............0023

     Backplane CPLD Revision.........0C

     Local CPLD image file...........BPN_CPLD.jed

     Uploading FW...Done

     Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Don

n

Status: Backplane CPLD is updated for 192.168.34.56
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateBackplaneCpld --update_list 0:BPN_CPLD.jed,1:BPN_CPLD.jed --
manual_ejected
```

The console output contains the following information.

```
Status: Start updating Backplane CPLD for 192.168.34.56

************************************WARNING****************************

    Do not remove AC power from the server.

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

Warning: All drives on backplane will be force ejected due to backplane
reset after update.


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

     Backplane CPLD ID...............0023
     Backplane CPLD Revision.........0C

     Local CPLD image file..........BPN_CPLD.jed

     Uploading FW...Done

     Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Don

n

     Backplane CPLD ID...............0023

     Backplane CPLD Revision.........0C

     Local CPLD image file..........BPN_CPLD.jed

     Uploading FW...Done

     Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Don

n


Status: Backplane CPLD is updated for 192.168.34.56
```

Notes:

- This command is only available on X12/H12 and later platforms with storage backplanes installed.
- A maximum of four backplane CPLDs can be updated.

5.20 PCIeSwitch Management for a Single System

5.20.1 Getting PCIeSwitch Information

Use the "GetPCIeSwitchInfo" command to get and read the PCIeSwitch information of the managed system and parse PCIeSwitch information from the firmware file.

Syntax:

```
sum -c GetPCIeSwitchInfo [--file <filename> [--file_only]]
```

Example:

In-Band:

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

In-Band:

```
[SUM_HOME]# ./sum -c GetPCIeSwitchInfo --file fw_file.img --file_only
```

- The console output contains the following information for the Broadcom chipset on the H12DGQ-NT6 system.

```
Managed system..........................localhost
PCIe Switch Device Vendor...............Microchip
    Device ID...........................0
    Device Name.........................SwitchPlx0
    Pex Cfg Version.....................1209
    Device ID...........................1
    Device Name.........................SwitchPlx1
    Pex Cfg Version.....................1209
    Device ID...........................2
    Device Name.........................SwitchPlx2

    Pex Cfg Version.....................3407

    Device ID...........................3

    Device Name.........................SwitchPlx3

    Pex Cfg Version.....................3407


Local Firmware File....................H12DGQ_NT6_1207_PWR.bin

PCIe Switch Device Vendor...............Broadcom

    Pex Cfg Version.....................1207
```

- The console output contains the following information for the Microchip chipset on a X12DSC-6 motherboard that includes AOM-S3616-S/AOM-SADPT-S.

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

PCIe Switch Device Vendor...............Microchip

    Device ID...........................0

    Device Name.........................switchtec0

    FW Version..........................3.60 B049

    CFG CRC.............................101a194c


Local Firmware File....................MCH036B360049_20201210.fwimg

PCIe Switch Device Vendor...............Microchip

    Generation..........................GEN4
```

```
Type................................CFG

Version.............................3.60 B049

Image Length........................267768 bytes

CRC.................................101a194c

Secure Version......................00000000
```

Notes:

- This command is available on H12DGQ-NT6 with Broadcom PCIeSwitch Gen4 Series chipsets and X12DSC-6 with Microchip PCIeSwitch Gen4 Series chipsets platforms.
- On the H12DGQ-NT6 platform with Broadcom PCIeSwitch Gen4 Series chipsets, find the readme.txt in the "SUM/driver/broadcom/PlxSdk" folder to load the device driver.
- On the X12DSC-6 platform with Microchip PCIeSwitch Gen4 Series chipsets, download the SDK from Microsemi and follow the instructions on the website to load the device driver.

5.20.2 Updating the PCIeSwitch Firmware Image

Use the “UpdatePCIeSwitch” command with the PCIeSwitch firmware image to update the PCIeSwitch firmware of a managed system.

Syntax:

```
sum -c UpdatePCIeSwitch --dev_id <index> --file <filename>
```

Example:

In-band:

```
[SUM_HOME]# ./sum -c UpdatePCIeSwitch --file fw_file.img --dev_id 0
```

- The console output contains the following information for a Broadcom chipset on an H12DGQ-NT6 system.

```
Managed system..........................localhost
PCIe Switch Device Vendor...............Broadcom
    Device ID...........................0
    Device Name.........................SwitchPlx0
    Pex Cfg Version.....................1207


Local Firmware File......................H12DGQ_NT6_1209_PWR.bin
PCIe Switch Device Vendor................Broadcom
    Pex Cfg Version......................1209
Update firmware progress Started ...
Writing Firmware ........................(100%)
Update firmware progress Finished.
Update firmware success.
```

- The console output contains the following information for Microchip chipset on X12DSC-6 systems with AOM-S3616-S/AOM-SADPT-S.

```
Managed system..........................localhost
PCIe Switch Device Vendor...............Microchip
    Device ID...........................0
    Device Name.........................switchtec0
    FW Version..........................3.60 B049
    CFG CRC.............................101a194c


Local Firmware File.....................MCH036B360049_20201210.fwimg
PCIe Switch Device Vendor...............Microchip
    Generation..........................GEN4
    Type................................CFG
    Version.............................3.60 B049
    Image Length........................267768 bytes
    CRC.................................101a194c
    Secure Version......................00000000


Update firmware progress Started ...
Writing Firmware ...................... (100%)
```

```
Update firmware progress Finished.

Update firmware success.

Note: Please reboot the system to activate the updated image.
```

Notes:

- This command is available on H12DGQ-NT6 with Broadcom PCIeSwitch Gen4 Series chipsets and X12DSC-6 platforms with Microchip PCIeSwitch Gen4 Series chipsets.
- On H12DGQ-NT6 platforms with Broadcom PCIeSwitch Gen4 Series chipsets, find the readme.txt in the "SUM/driver/broadcom/PlxSdk" folder to load the device driver.
- On X12DSC-6 platforms with Microchip PCIeSwitch Gen4 Series chipsets, download the SDK from Microsemi and follow the instructions on the website to load the device driver.

5.21 Virtual Media Management for a Single System

Starting from SUM 2.11.0 for platforms that support multiple virtual media devices, use the “GetVmInfo” and “VmManage” commands to use virtual media features. For platforms that only support a single virtual media device, use the “MountIsoImage,” “UnMountIsoImage,” “MountFloppyImage” and “UnmountFloppyImage” commands to mount and unmount an image.

See the table below for the virtual media features.

Command	SUM 2.11.0 and later	
	Platforms only support single virtual media device	Platforms support multiple virtual media devices
GetVmInfo	No support	Support
VmManage (Action: Enable/Disable)	Support	Support
VmManage (Action: Mount/Unmount)	No support	Support
MountIsoImage	Support	No support
UnmountIsoImage	Support	No support
MountFloppyImage	Support	No support
UnmountFloppyImage	Support	No support

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

Use the “MountIsoImage” command to mount an ISO image as a virtual media to the managed system through a SAMBA/HTTP/HTTPS server. Since SUM 2.5.0, SUM has a new rule when using new special characters for virtual media. For more details, see the tables below. Starting from SUM 2.11.0, this command is only supported on the platforms that only support a single virtual media device.

HTTP/HTTPS URL format:

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

SAMBA URL/UNC format:

SAMBA URL	smb://<hostname or IP>/<file path> smb://<hostname or IP>:<port number>/<file path> smb://<hostname or IP>/<shared point>/<file path>

	smb://<hostname or IP>:<port number>/<shared point>/<file path>
SAMBA UNC	\\<hostname or IP>\<file path> \\<hostname or IP>:<port number>\<file path> \\<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> or <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) or . (a period)
- 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.
- IPv6 link-local address starts with fe80 is not allowed.

Syntax:

```
sum [-i <IP or host name> | [-I Redfish_HI]] [-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 'https://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 'https://[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
'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd

[SUM_HOME]# ./sum -c MountIsoImage  --image_url
'https://[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) or . (a period)
- 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 ^ (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.
- IPv6 link-local address starts with fe80 is not allowed.

5.21.2 Removing an ISO Image as Virtual Media

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

Starting from SUM 2.11.0, this command is only supported on platforms that support a single virtual media device only.

Syntax:

```
sum [-i <IP or host name> | [-I Redfish_HI]] [-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
```

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

Use the “MountFloppyImage” command to have SUM mount a binary floppy image to the managed system virtually. Starting from SUM 2.11.0, this command is only supported on platforms that support a single virtual media device only.

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: The floppy image size should be 1.44MB.

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

Use the “UnmountFloppyImage” command to execute SUM to virtually remove a binary floppy image from the managed system. Starting from SUM 2.11.0, this command is only supported on platforms that support single virtual media device only.

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.

5.21.5 Get Virtual Media Information from the Managed System

For platforms that support multiple virtual media devices, use the “GetVmInfo” command to get the virtual media information from the managed system.

Syntax:

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

Example:

OOB:

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

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

In-Band:

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

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c GetVmInfo --dev_id 2
```

The console output contains the following information if the platform is supported to manage multiple virtual media devices.

```
Supermicro Update Manager (for UEFI BIOS) 2.11.0 (2023/03/23) (x86_64)

Copyright(C) 2013-2023 Super Micro Computer, Inc. All rights reserved.



Status: Start to get virtual media information.



Virtual Media Information

=============================
    Device 1

    ============

        Device status: Unmounted

        Media type: N/A

        Connection setting: NotConnected

        Image: N/A

        SSL certificate verified: N/A

        Self-signed certificate accepted: N/A

        UserName: N/A


    Device 2

    ============

        Device status: Unmounted

        Media type: N/A

        Connection setting: NotConnected

        Image: N/A

        SSL certificate verified: N/A

        Self-signed certificate accepted: N/A

        UserName: N/A


    Device 3
```

```
    ============

        Device status: Unmounted

        Media type: N/A

        Connection setting: NotConnected

        Image: N/A

        SSL certificate verified: N/A

        Self-signed certificate accepted: N/A

        UserName: N/A
```

The console output contains the following information if the platform is supported to manage multiple virtual media devices and the device is mounted by iKVM. Additionally, it should be noted that if the device is mounted by iKVM, it can only be unmounted by iKVM.

```
Supermicro Update Manager (for UEFI BIOS) 2.11.0 (2023/03/23) (x86_64)

Copyright(C) 2013-2023 Super Micro Computer, Inc. All rights reserved.


Status: Start to get virtual media information.


Virtual Media Information

=============================

    Device 1

    ============
        Device status: Mounted

        Media type: Floppy

        Connection setting: Applet

        Image: kvm_floppy
```

5.21.6 Managing Multiple Virtual Media Devices from the Managed System

For platforms that support multiple virtual media devices, use the “VmManage” command with the Mount/Unmount option to mount or unmount an image. Use the “VmManage” command with the --action Enable/Disable option to enable or disable virtual media on all platforms. For the accepted URL format, please refer to *5.19.1 Providing an ISO Image as a Virtual Media through BMC and File Server*. This command supports up to three virtual media devices, including ISO and floppy images. For the detailed usages, please refer to the below.

- **For the Enable/Disable Action:**

  Use the “--action Enable/Disable” option to enable/disable virtual media from BMC.

  - The --port option is optional for the Enable/Disable action. If user provides --port option, SUM will configure virtual media port of BMC.

- **For the Mount Action:**

  Use the “--action Mount” option to mount an image on the image file server to specified virtual media device of BMC.

  - Use the --image_url option to specify the URL to access the shared image file.
  - Use the --id option to specify the ID to access the shared image file.
  - Use the --pw/--pw_file option to specify the password to access the shared image file.
  - Use the --dev_id option to specify the device ID of specified device.
  - The --verify_cert option is optional. If this option is used, SUM will verify SSL certificate. Only HTTPS protocol is supported.
  - The --accept_self_signed option is optional. If this option and the --verify_cert option are used, SUM will verify the self-signed SSL certificate. Only HTTPS protocol is supported.

- **For the Unmount Action:**

  Use the “--action Unmount” option to unmount the images from the specified virtual media device of the BMC.

  - Use the --dev_id option to specify the device ID of a specific device.

Syntax:

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
VmManage --action <Enable/Disable> [--port <port>]
```

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
VmManage --action Mount [--dev_id <device ID>] --image_url <URL> [[--id <id for
URL> --pw [password for URL]]|[--id <id for URL> --pw_file <password file
path>]] [--verify_cert [--accept_self_signed]]
```

```
sum [-i <IP or host name> | -I Redfish_HI] -u <username> -p <password> -c
VmManage --action Unmount [--dev_id <device ID>]
```

Example:

OOB:

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Enable --port 623

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Disable --port 623

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id
smbid --pw smbpasswd --dev_id 1

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso' --id
smbid --pw smbpasswd --dev_id 2

[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id
smbid --pw smbpasswd --dev_id 3

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

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id
smbid --pw smbpasswd --verify_cert --accept_self_signed --dev_id 2
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'https://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --
id smbid --pw_file smbpasswd.txt --verify_cert --accept_self_signed --dev_id 3
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url '\\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id smbid -
-pw_file smbpasswd.txt --dev_id 1
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url '\\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id smbid --
pw_file smbpasswd.txt --dev_id 2
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Unmount --dev_id 1
```

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --action
Unmount --dev_id ALL
```

```
smbpasswd.txt:

smbpasswd
```

In-band:

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Enable
--port 623
```

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Disable --port 623
```

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Mount
--image_url 'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --
pw smbpasswd --dev_id 1

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Mount
--image_url 'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso' --id smbid --
pw smbpasswd --dev_id 2

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Mount
--image_url 'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --
pw smbpasswd --dev_id 3

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Mount
--image_url 'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id
smbid --pw_file smbpasswd.txt --dev_id 1

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Mount
--image_url 'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid -
-pw smbpasswd --verify_cert --accept_self_signed --dev_id 2

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Mount
--image_url 'https://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id
smbid --pw_file smbpasswd.txt --verify_cert --accept_self_signed --dev_id 3

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Mount
--image_url '\\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id smbid --
pw_file smbpasswd.txt --dev_id 1

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action Mount
--image_url '\\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id smbid --
pw_file smbpasswd.txt --dev_id 2

[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Unmount --dev_id 1
```

```
[SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Unmount --dev_id ALL
```

```
smbpasswd.txt:
smbpasswd
```

Notes:

- Special characters for ID and password: ^ (a caret)
- Special characters for shared host: - (a dash) or . (a period)
- 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.
- IPv6 link-local address starts with fe80 is not allowed.
- The maximum ISO image is 10 GB.
- The floppy image size should be 1,474,560 bytes.
- Up to three virtual media devices are supported, including ISO and floppy images.
- If the device is mounted by iKVM, the device can only be unmounted by iKVM.

6 Managing Multiple Systems

For managing multiple systems, SUM provides the "-l" option to concurrently execute commands on multiple systems enumerated in a system list file.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c <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.

```
   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 to the command line to execute the GetDmiInfo command. 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.

Multiple Systems Remote In-Band Syntax:

```
sum [-I Remote_INB | -I Remote_RHI] -l <system list file> -c <command> [command options]
```

The managed systems should be enumerated row-by-row in the system list file. Two formats are supported for Remote In-Band (Remote_INB) as follows.

```
   Format 1: OS_IP_or_HostName OS_Username OS_Password
   Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey OS_Privatekey_Password
```

Two formats are supported for Remote Redfish Host Interface (Remote_RHI) as follows.

```
   Format 1: OS_IP_or_HostName OS_Username OS_Password BMC_Username BMC_Password
   Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey OS_Privatekey_Password
BMC_Username BMC_Password
```

The options --oi, --ou, --op, --os_key, --os_key_pw, -u, and -p must be specified in the system list file for Multiple Systems Remote In-band usage.

Example:

```
[SUM_HOME]# ./sum [-I Remote_INB | -I Remote_RHI] -l SList.txt -u ADMIN -p
PASSWORD -c GetBmcInfo

SList.txt for Remote_INB:
    192.168.34.56 root 111111
    192.168.34.57 root /root/pvt_key 111111

SList.txt for Remote_RHI:
    192.168.34.56 root 111111 ADMIN PASSWORD
    192.168.34.57 root /root/pvt_key 111111 ADMIN PASSWORD
```

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 use of commands that take input files as arguments, such as the UpdateBios command, see *6.1.1 File Input* for its usage.

Notes:

- For the ActivateProductKey command, different formats are used. Refer to *6.2.1 Activating Multiple Managed Systems*.
- For the SetBiosPassword command, different formats are used. Refer to *6.4.12 Setting BIOS Administrator Password.*
- For the RemoteExec command, different formats are used. Refer to *6.8.12 Remote Execution.*
- For the CpuOnDemand command, different formats are used. Refer to *6.3.8 Getting and activating CpuOnDemand function* for the action of 2,3 and 4.
- Repeated managed system IPs or names in system list file are not allowed.
- SUM limits its maximum concurrent executiong 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
Supermicro_BIOS.rom
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

In this example, SUM uses the input file Supermicro_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 onscreen, is the system list file name appended by ".log_", "yyyy-mm-dd_hh-mm-ss" (date and time) and "_PID" (process ID). In the log file, the information of each system is listed in the "Last Update Time", "Execution parameters", "Summary", and "Status List" sections. The "Execution Message" section only lists the . The following example shows the log file SList.txt.log_2013-10-02_15:57:40_7370 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 Getting 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
```

The "-u" and "-p" options are required to specified in the command line for Format 1. The -u and -p options can be removed from the command line for Format 2. In addition, the Username/Password in the system list file overwrites the -u and -p options in the command line. If the --key option is specified in the command line, the exception will be thrown. If you use the "--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":"11111111111111111111222222222222222333333
    33333333abababababababababababababbabcdcdcdcdcdcdccdcdcddcdefefefefefefefeefefefefghgh
    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 “ActivateProductKey” command. 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 “ActivateProductKey” command. 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 “QueryProductKey” command.

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 "CheckOOBSupport" command 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 "CheckAssetInfo" command 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 “CheckSensorData” command 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 “CheckSystemUtilization” command 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 “ServiceCalls” command 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.

6.3.6 Monitoring and Controlling PFA of the System

Use the “SystemPFA” command to monitor and set the predictive failure analysis function of BIOS on the managed system. The message output will be the same as that in *5.2.6 Monitoring and Controlling PFA of the System (Single System)*.

Syntax:

```
sum -l < system list file > [-u <username> -p <password>] -c SystemPFA --action
<action>] [--reboot] [--post_complete]
```

Option Commands	**Descriptions**
--action	Sets action to: 1 = GetCurrentStatus 2 = Enabled 3 = Disabled

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SystemPFA --action Enable
--reboot --post_complete
```

```
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.

6.3.7 Monitoring and Checking Memory Health of the System

Use the "MemoryHealthCheck" command to access the function in BIOS to check memory health of the managed system. The message output will be the same as that in *5.2.7 Checking Memory Health of the Managed System (Single System)*.

Syntax:

```
sum -l < system list file > [-u <username> -p <password>] -c MemoryHealthCheck -
-action <action> --reboot [--post_complete]
```

Option Commands	Descriptions
--action	Sets action to: 1 = GetCurrentStatus 2 = Persistent 3 = Enable 4 = Disable

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MemoryHealthCheck --
action Persistent --reboot --post_complete

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.

6.3.8 Getting and Activating the CpuOnDemand Function

Use the "CpuOnDemand" command to activate and check Intel® On Demand Capabilities of the managed system. The message output will be the same as that in 5.2.8 Getting and activating CpuOnDemand function (Single System).

The command provides the following actions:

Option Commands	Descriptions
--action	Sets action to: 1 = GetHwInfo 2 = GetOnDemandState 3 = SetLicenseActivateCode 4 = EnablePPIN

1. The syntax of GetHwInfo:

```
sum -l <system list file> [-u <username> -p <password>] -c CpuOnDemand --action
GetHwInfo [--file < mlist_hw_id_file_name>] [--overwrite]
```

The format of the system list file is the same as that explained in 6. Managing Multiple Systems.
For the output of --file, the format is the same as that explained in 5.2.8.2 CpuOnDemand command usage

2. The syntax of GetOnDemandState:

```
sum -l <system list file> [-u <username> -p <password>] -c CpuOnDemand --action
GetOnDemandState [--file < mlist _StateReport>] [-v] [--squash] [--overwrite]
```

The system list file is another format that requires PPIN appended in each row. If the system has more than one CPU, one row only allows one PPIN so that system should have multiple lines to indicate different PPINs. There are two formats supported.

```
Format 1: BMC_IP_or_HostName PPIN
Format 2: BMC_IP_or_HostName Username Password PPIN
```

The “-u” and “-p” options are required to specified in the command line for Format 1. The -u and -p options can be removed from the command line for Format 2. In addition, the Username/Password in the system list file overwrites the -u and -p options in the command line.

Example:

```
[SUM_HOME]# ./sum -l SList.txt -c CpuOnDemand --action GetOnDemandState --file
mlist_report.txt
```

```
SList.txt:
    192.168.34.56 AABBCCDD00112233
    192.168.34.57 ADMIN1 PASSWORD1 EEFFGGHH00112233
    192.168.34.57 ADMIN1 PASSWORD1 EEFFGGHH00445566
```

3. The syntax of SetLicenseActivateCode:

```
sum -l <system list file> [-u <username> -p <password>] -c CpuOnDemand --action
SetLicenseActivateCode --lac_file <LAC+.txt> [--reboot] [--post_complete]
```

The format of the system list file is the same as that explained in action 1 = GetHwInfo.

4. The syntax of EnablePPIN:

```
sum -l <system list file> [-u <username> -p <password>] -c CpuOnDemand --action
EnablePPIN --reboot [--post_complete]
```

The format of the system list file is the same as that explained in action 1 = GetHwInfo.

6.3.9 Getting and Clearing the Chassis Intrusion Status for the Managed System

Use the "ChassisIntrusion" command to get and clear the status of the chassis intrusion sensor. If a hardware intrusion is detected, the status will be "Hardware Intrusion", otherwise, it will be "Normal". This command can be used to get the status or clear the status to "Normal". The message output will be the same as that in *5.2.9. Getting and Clearing the chassis intrusion status for the manahed system.*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChassisIntrusion --
action <action>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChassisIntrusion --action
Status
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the execution "Status" field for a managed system is SUCCESS, the chassis intrusion information of the managed system will be shown in the "Execution Message" section of the managed system in the created log file.

6.3.10 Managing FRU Information

6.3.10.1 Getting FRU Information

Use the “GetFruInfo” command to get or dump the FRU information on the managed system and read FRU information from the local FRU file. The message output will be the same as that in 5.2.9.1 Getting FRU information (Single System).

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetFruInfo [--file
<filename> [--dump] | [--file_only]] [--overwrite] [--dev_id <Device ID>] | [--
showall]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetFruInfo --file
dumpedFile --dump

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetFruInfo --dev_id 1,2

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetFruInfo --showall

SList.txt:
    192.168.34.56
    192.168.34.57
```

If you execute the GetFruInfo command for 192.168.34.56 and 192.168.34.57, SUM will create dumpedFile.192.168.34.56 and dumpedFile.192.168.34.57, respectively.

6.3.10.2 Restoring FRU Information

Use the “RestoreFruInfo” command to restore the FRU information on the managed system. The message output will be the same as that in 5.2.9.2 Restoring FRU information (Single System).

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c RestoreFruInfo --file
<filename> [--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c RestoreFruInfo --file
dumpedFile --individually
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If you want to restore 192.168.34.56 and 192.168.34.57, you need to provide two files: dumpedFile.192.168.34.56 and dumpedFile.192.168.34.57. Then set the --file argument with the “dumpedFile” file name. With the --individually option, SUM searches for dumpedFile.192.168.34.56 and dumpedFile.192.168.34.57 to restore 192.168.34.56 and 192.168.34.57, respectively.

6.3.10.3 Changing FRU Information

Use the “ChangeFruInfo” command to change the FRU information on the managed system. The message output will be the same as that in *5.2.10.3 Changing FRU Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeFruInfo --item
<item name> --value <assignment value>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeFruInfo --item CT -
-value 0x01
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.4 BIOS Management for Multiple Systems

6.4.1 Getting BIOS Firmware Image Information

Use the “GetBiosInfo” command to get 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).*

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBiosInfo [--file
<filename> [--showall]
```

Multiple Systems Remote In-Band Syntax:

```
Sum [-I Remote_INB | -I Remote_RHI] -l <system list file> -c GetBiosInfo [--file
<filename> [--showall] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBiosInfo --file
Supermicro_BIOS.romSList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetBiosInfo --file
Supermicro_BIOS.rom
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

ⓘ **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 "UpdateBios" command with the BIOS firmware image Supermicro_BIOS.rom or bios_image.tar for OpenBMC 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)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateBios --file
<filename> [options…]
```

Multiple Systems Remote In-Band Syntax:

```
sum [-I Remote_INB | -I Remote_RHI] -l <system list file> [-u <username> -p
<password>] -c UpdateBios --file <filename> [--remote_sum <remote sum path>]
[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.
--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:

Multiple System OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBios --file
Supermicro_BIOS.rom
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c UpdateBios --file
Supermicro_BIOS.rom
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

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 Getting Current BIOS Settings

Use the “GetCurrentBiosCfg” command 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 Getting Current BIOS Settings (Single System)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetCurrentBiosCfg --
file <USER_SETUP.file> [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [--overwrite]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_INB -l <system list file> -c GetCurrentBiosCfg --file
<USER_SETUP.file> [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [--overwrite] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetCurrentBiosCfg --file
USER_SETUP.file
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetCurrentBiosCfg --file
USER_SETUP.file
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD current_password
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password current_password
```

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 Getting 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 ChangeBiosCfg command 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 "ChangeBiosCfg" command, see the note in *5.3.4 Updating BIOS Settings Based on the Current BIOS Settings (Single System)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeBiosCfg --file
<USER_SETUP.file> [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [--reboot] [--individually]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_INB -l <system list file> -c ChangeBiosCfg --file
<USER_SETUP.file> [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [--reboot] [--individually] [--remote_sum <remote
sum path>]
```

Example:

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c ChangeBiosCfg --file
USER_SETUP.file --reboot

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD current_password
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password current_password
```

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 Getting Factory BIOS Settings

Use the “GetDefaultBiosCfg” command 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.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetDefaultBiosCfg --
file <USER_SETUP.file> [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [--overwrite]
```

Multiple Systems Remote In-Band Syntax:

```
Sum -I Remote_INB -l <system list file> -c GetDefaultBiosCfg --file
<USER_SETUP.file> [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [--overwrite] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetDefaultBiosCfg --file
USER_SETUP.file
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD current_password
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password current_password
```

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 --overwrite option 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 Getting 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 “LoadDefaultBiosCfg” command 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.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultBiosCfg
[[--current_password <current password>] | [--cur_pw_file <current password file
path>]] [--reboot]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_INB -l <system list file> -c LoadDefaultBiosCfg [[--
current_password <current password>] | [--cur_pw_file <current password file
path>]] [--reboot] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBiosCfg --
reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c LoadDefaultBiosCfg --reboot

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD current_password
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password current_password
```

6.4.8 Getting DMI Information

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetDmiInfo --file
<DMI.txt>  [--overwrite]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Redish_HI -l <system list file> -c GetDmiInfo --file <DMI.txt>  [--
overwrite] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetDmiInfo --file DMI.txt --
overwrite
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

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 “EditDmiInfo” command to edit the editable DMI items. For details on the “EditDmiInfo” command, refer to *5.3.9 Editing DMI Information (Single System)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c EditDmiInfo --file
<DMI.txt> [--item_type <Item Type> --item_name <Item Name> | --shn <Item Short
Name>] [--value <Item Value> | --default]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_INB -l <system list file> -c EditDmiInfo --file <DMI.txt> [--
item_type <Item Type> --item_name <Item Name> | --shn <Item Short Name>] [--
value <Item Value> | --default] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c EditDmiInfo --file DMI.txt --shn
SYVS --default
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

If the execution "Status" field for a managed system (e.g., 192.168.34.56) is "SUCCESS", its edited DMI information is 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 "ChangeDmiInfo" command 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 file.
- For detailed usage notes of the command "ChangeDmiInfo," see *5.3.10 Updating DMI Information*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeDmiInfo --file
<DMI.txt>  [--reboot] [--individually]
```

Multiple Systems Remote In-Band Syntax:

```
Sum -I Remote_INB -l <system list file> -c ChangeDmiInfo --file <DMI.txt>  [--
reboot] [--individually] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c ChangeDmiInfo --file DMI.txt --
reboot

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

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 “SetBiosAction” command 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 "SetBiosPassword" command to update a BIOS Administrator password. The information will be the same as that in 5.3.12 Setting Up a BIOS Administrator Password.

Multiple Systems OOB 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>] [--current_password <current password> | --
cur_pw_file <current password file path>]] [--reboot]
```

The managed systems should be enumerated row by row in the system list file. For the "SetBiosPassword" command from SUM 2.10.0, the system list file format is fixed for specific commands. Note that the New_BIOS_Password and Current_Password fields are both **REQUIRED**. If the managed system has been installed with a BIOS Administrator password, this field should be filled with the current BIOS Administrator password. If the managed system has no BIOS Administrator password installed, users should still fill this field with empty value. Two formats are supported as follows:

```
   Format 1: BMC_IP_or_HostName New_BIOS_Password Current_BIOS_Password

   Format 2: BMC_IP_or_HostName Username Password New_BIOS_Password
Current_BIOS_Password
```

For format 1, it is required to specify both "-u" and "-p" options in the command line.
For format 2, options "-u" and "-p" are optional in the command line. In this case, the Username/Password in the system list file overwrites the options "-u" and "-p" in the command line.

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_INB -l <system list file> -c SetBiosPassword [[[--new_password
<new password> --confirm_password <confirm password>] | --pw_file <password file
path>] [--current_password <current password> | --cur_pw_file <current password
file path>]] [--reboot] [--remote_sum <remote sum path>]
```

Two formats are supported for Multiple Remote In-Band as follow:

```
   Format 1: BMC_IP_or_HostName New_BIOS_Password Current_BIOS_Password

   Format 2: BMC_IP_or_HostName Username Password New_BIOS_Password
Current_BIOS_Password
```

SUM supports flexible usage to set and check the BIOS Administrator password when managing multiple systems as follows.

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 option "--new_password" or "--pw_file". If you assign option "--new_password" or "--pw_file" in command line, the option value will overwrite the value in system list file.

If you want to assign a different current BIOS Administrator password for current password checking, you can specify a Current_BIOS_Password corresponding to each system for Format 1 or Format 2 without using option "--current_password" or "--cur_pw_file". If you assign option "--current_password" and "--cur_pw_file" in command line, the option value will overwrite the value in system list file.

Example:

```
SList.txt:

    192.168.34.56 new_ pwd_11 current_pwd_11

    192.168.34.57 ADMIN1 PASSWORD1 new_pwd_22 current_pwd_22
```

To specify new password and current password corresponding to each system, you can use the example below with system list file SList.txt.

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBiosPassword
```

system	BMC user	BMC password	New BIOS password	Current BIOS password
192.168.34.56	ADMIN	ADMIN	new_ pwd_11	current_pwd_11
192.168.34.57	ADMIN1	PASSWORD1	new_pwd_22	current_pwd_22

To assign the same new password and current password with options --new_password and --current_password for every system in the system list file SList.txt, you can use the following example.

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBiosPassword --
new_password 12345678 --confirm_password 12345678 --current_password 654321
```

system	BMC user	BMC password	New BIOS password	Current BIOS password
192.168.34.56	ADMIN	ADMIN	12345678	654321
192.168.34.57	ADMIN1	PASSWORD1	12345678	654321

```
SList.txt:

    192.168.34.56 ADMIN3 PASSWORD3 new_ pwd_55 current_pwd_55

    192.168.34.57 ADMIN4 PASSWORD4 new_ pwd_66 current_pwd_66

passwd.txt:

    NewBiosPasswordString

Current_passwd.txt:

    CurrentBiosPasswordString
```

To assign the same new password and current password with options --pw_file and --cur_pw_file for every system in the system list file SList.txt, you can use the following example. In this case, options “-u” and “-p” are optional.

```
[SUM_HOME]# ./sum -l SList.txt -c SetBiosPassword --pw_file passwd.txt --
cur_pw_file current_passwd.txt
```

system	BMC user	BMC password	New BIOS password	Current BIOS password
192.168.34.56	ADMIN3	PASSWORD3	NewBiosPasswordString	current_pwd_55
192.168.34.57	ADMIN4	PASSWORD4	NewBiosPasswordString	current_pwd_66

Notes:

- The new uploaded password will only take effect after the managed systems reboot or power up.
- The SetBiosPassword command supports CSV format in the system list file. The CSV format uses spaces to separate values and double quotes to enclose values.
- To clear the BIOS Administrator password with the system list file, press the **spacebar** twice to skip entering the BIOS_new_passowrd. The format should be like this :

  ```
  BMC_IP_or_HostName  Current_Password
  BMC_IP_or_HostName Username Password  Current_Password
  ```
- For systems with no BIOS Administrator password installed, MUST leave one space symbol right after the New_BIOS_Password. The system list file format should be like this:

  ```
  BMC_IP_or_HostName New_BIOS_Password
  BMC_IP_or_HostName Username Password New_BIOS_Password
  ```

6.4.13 Managing BIOS RoT Functions

Use the “BiosRotManage” command to manage RoT fuctions. For details, see *5.3.14 Managing BIOS RoT Functions (Single System)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c BiosRotManage --
action <action> [--file <evidence.bin.gz>] [--overwrite] [--reboot]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_RHI -l <system list file> -c BiosRotManage --action <action> [--
file <evidence.bin.gz>] [--overwrite] [--reboot] [--remote_sum <remote sum
path>]
```

Example:

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c BiosRotManage --action
UpdateGolden --reboot

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

6.4.14 Seamless Update Capsule File

- **Seamless Update feature in UpdateBios command**

Use the “UpdateBios” command with --file <CAPSULE_FILE.bin> to update capsule file to a managed system. For details, see *5.3.15 Seamless Update Capsule File (Single System)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> -u <username> -p <password> -c UpdateBios --file
<CAPSULE_FILE.bin> [--staged update] [--reboot] [--post_complete]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_RHI -l <system list file> -c UpdateBios --file <CAPSULE_FILE.bin>
[--staged update] [--reboot] [--post_complete] [--remote_sum <remote sum path>]
```

Example:

```
Multiple Systems OOB:
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBios --file
CAPSULE_FILE.bin --reboot --post_complete

SList.txt:
    192.168.34.56
    192.168.34.57

Multiple Systems Remote In-Band through Redfish Host Interface:
[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c UpdateBios --file
CAPSULE_FILE.bin --reboot --post_complete

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

- **Getting capsule information in GetBiosInfo command**

Use the “GetBiosInfo” command with --file <CAPSULE_FILE.bin> to get capsule information on a managed system and local capsule file. For details, see 5.3.15 Seamless Update Capsule File (Single System).

Multiple Systems OOB Syntax:

```
sum -l <system list file> -u <username> -p <password> -c GetBiosInfo --file
<CAPSULE_FILE.bin> [--showall]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_RHI -l <system list file> -u <username> -p <password> -c
GetBiosInfo --file <CAPSULE_FILE.bin> [--showall] [--remote_sum <remote sum
path>]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBiosInfo --file
CAPSULE_FILE.bin --showall

SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band through Redfish Host Interface
:

```
[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c GetBiosInfo --file
CAPSULE_FILE.bin --showall

Slist.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

6.4.15 Getting SCP Firmware Image Information

Use the "GetScpInfo" command to get the SCP firmware image information from the managed systems as well as the input SCP firmware image. The message output will be the same as that in *5.3.16 Getting SCP Image Information (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetScpInfo
```

Example:

```
[SUM_HOME]# ./sum -l Slist.txt -u ADMIN -p PASSWORD -c GetScpInfo
```

```
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.

6.4.16 Updating the SCP Firmware Image

Use the “UpdateScp” command with the SCP firmware image scp_image.tar to update managed systems. For details on the “UpdateScp” command, see the usage notes in *5.3.17 Updating the SCP Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateScp --file
<filename> --reboot
```

Example:

```
[SUM_HOME]# ./sum -l Slist.txt -u ADMIN -p PASSWORD -c UpdateScp --file
scp_image.tar
```

```
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.

6.4.17 Getting Fixed Boot Settings

Use the “GetFixedBootCfg” command to get the current Fixed Boot settings from the managed systems and save them in the output files individually for each managed system enumerated in the system list file. For details on the “GetFixedBootCfg” command, see *5.3.18 Getting Fixed Boot Setting (Single System)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetFixedBootCfg --
file <USER_SETUP.file> [--overwrite] --redfish
```

Example:

```
Multiple Systems OOB:
[SUM_HOME]# ./sum -l Slist.txt -u ADMIN -p PASSWORD -c GetFixedBootCfg --file
USER_SETUP.file --overwrite --redfish

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 --overwrite option 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.

6.4.18 Updating Fixed Boot Settings

To update the fixed boot settings, follow these steps:

1. Select one managed system as the golden sample for the current fixed boot settings.
2. Follow the steps in 5.3.19 Updating Fixed Boot Setting for that system.
3. Edit the item/variable values in the user setup file USER_SETUP.file to the desired values as illustrated in *4.15 Fixed Boot Configuration XML File Format*.

4. Use the ChangeFixedBootCfg command with the modified USER_SETUP.file to update the fixed boot configurations for managed systems.

- **Note:** Use the --individually option to update each managed system with the corresponding configuration file.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeFixedBootCfg --
file <USER_SETUP.file> [--reboot] [--individually] --redfish
```

Example:

```
Multiple Systems OOB:
[SUM_HOME]# ./sum -l Slist.txt -u ADMIN -p PASSWORD -c ChangeFixedBootCfg --file
USER_SETUP.file --reboot --redfish

[SUM_HOME]# ./sum -l Slist.txt -u ADMIN -p PASSWORD -c ChangeFixedBootCfg --file
USER_SETUP.file --reboot --individually --redfish

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.

6.4.19 Managing a Secure Boot

Use the “SecureBootManage” command to manage a secure boot. This command can be used to get or set secure boot status to “Enabled/Disabled” and also to upload or delete secure boot keys.

For details, see *5.3.18 Managing secure boot (Single System)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SecureBootManage --
redfish --action <action> [--file_type <file type>] [--file <CertificateFile>]
[--individually]] [--reboot [--post_complete]]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_RHI -l <system list file> -c SecureBootManage --redfish --action
<action> [--file_type <file type>] [--file <CertificateFile>] [--individually]
[[--reboot [--post_complete]]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l Slist.txt -u ADMIN -p PASSWORD -c SecureBootManage --
redfish --action UploadCertificate --file_type PK --file CertificateFile.pem --
individually --reboot --post_complete
```

```
Slist.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -l Slist.txt -c SecureBootManage --redfish --
action UploadCertificate --file_type PK --file CertificateFile.pem --
individually --reboot --post_complete
```

```
Slist.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

6.5 BMC Management for Multiple Systems

6.5.1 Getting BMC Firmware Image Information

Use the “GetBmcInfo” command to get 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 for Getting BMC Firmware Image Information from Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBmcInfo [--file
<filename>] [--file_only] [--extract_measurement] [--showall]
```

Syntax for Getting BMC Firmware Image Information from Multiple Systems Remote In-Band:

```
sum [-I Remote_INB | -I Remote_RHI] -l <system list file> -c GetBmcInfo [--file
<filename>] [--file_only] [--extract_measurement] [--remote_sum <remote sum
path>] [--showall]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBmcInfo --file
Supermicro_BMC.rom
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetBmcInfo --file
Supermicro_BMC.rom
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

```
[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c GetBmcInfo --file
Supermicro_BMC.rom
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

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 “UpdateBmc” command with BMC firmware image Supermicro_BMC.rom or bmc_image.tar for OpenBMC to update managed systems. For details on the “UpdateBmc” command, see the usage notes in *5.4.2 Updating the BMC Image (Single System)*.

Syntax for Updating BMC Firmware Images on Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateBmc --file
<filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--
overwrite_ssl]
```

Syntax for Updating the BMC Firmware Images on Multiple Systems through Remote In-Band:

```
sum [-I Remote_INB | -I Remote_RHI] -l <system list file> -c UpdateBmc --file
<filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--
overwrite_ssl] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBmc --file
Supermicro_BMC.rom

SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c UpdateBmc --file
Supermicro_BMC.rom

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password

[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c UpdateBmc --file
Supermicro_BMC.rom

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

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 Getting BMC Settings

Use the “GetBmcCfg” command to get or dump 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 details on the “GetBmcCfg” command, see the usage notes in *5.4.3 Getting BMC Settings (Single System)*.

Syntax for Getting the BMC Settings on Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBmcCfg --file <
BMCCfg.xml|BMCCfg.bin>  [--dump] [--overwrite]
```

Syntax for Getting the BMC Settings on Multiple Systems through Remote In-Band:

```
Sum [-I Remote_INB | -I Remote_RHI] -l <system list file> -c GetBmcCfg --file <
BMCCfg.xml|BMCCfg.bin>  [--dump] [--overwrite]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBmcCfg --file
BMCCfg.xml --overwrite

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBmcCfg --file
BMCCfg.bin --dump --overwrite

SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetBmcCfg --file BMCCfg.xml --
overwrite

[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetBmcCfg --file BMCCfg.bin --
dump --overwrite

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

Multiple Systems Remote In-Band through Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c GetBmcCfg --file BMCCfg.xml --
overwrite
```

```
[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c GetBmcCfg --file BMCCfg.bin --
dump --overwrite
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

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 or BMCCfg.bin.192.168.34.56. The option --overwrite is used to force the overwrite the existing file, e.g., BMCCfg.xml.192.168.34.56 or 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 Getting 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 "ChangeBmcCfg" command 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 for Updating the BMC Settings on Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeBmcCfg --file
<BMCCfg.xml|BMCCfg.bin >  [--restore] [--individually]
```

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_INB -l <system list file> -c ChangeBmcCfg --file
<BMCCfg.xml|BMCCfg.bin >  [--restore] [--individually] [--remote_sum <remote sum
path>]
```

Example:

Multiple Systems OOB:

```
[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.bin --restore

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcCfg --file
BMCCfg.xml --individually

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcCfg --file
BMCCfg.bin --restore --individually

SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c ChangeBmcCfg --file BMCCfg.xml -
-individually

[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c ChangeBmcCfg --file BMCCfg.bin -
-restore --individually

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

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.
If you want to restore 192.168.34.56 and 192.168.34.57, you need to provide two files: BMCCfg.bin.192.168.34.56 and BMCCfg.bin.192.168.34.57. Then set the argument --file with the

BMCCfg.bin file name. With the --individually option, SUM searches for BMCCfg.bin.192.168.34.56 and BMCCfg.bin.192.168.34.57 to restore 192.168.34.56 and 192.168.34.57 respectively.

6.5.5 Setting Up the BMC User Password

Use the "SetBmcPassword" command 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).

Multiple Systems OOB 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.

Multiple Systems Remote In-Band Syntax:

```
sum -I Remote_INB -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>]] [--remote_sum <remote sum 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
```

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 Getting the BMC KCS Privilege Level

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

Syntax for Getting the BMC KCS Privilege Levels from Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c GetKcsPriv
```

Syntax for Getting the BMC KCS Privilege Levels from Multiple Systems through Remote In-Band:

```
sum -I Remote_INB -l <system list file> -c GetKcsPriv [--remote_sum <remote sum
path>]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetKcsPriv

SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetKcsPriv

SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

6.5.7 Setting the BMC KCS Privilege Level

Use the “SetKcsPriv” command 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 "LoadDefaultBmcCfg" command 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 for Resetting BMC of Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c LoadDefaultBmcCfg [--
preserve_user_cfg] [--clear_user_cfg [--load_unique_password | --
load_default_password]]
```

Syntax for Resetting BMC of Multiple Systems through Remote In-Band:

```
sum -I Remote_INB -l <system list file> -c LoadDefaultBmcCfg [--
preserve_user_cfg] [--clear_user_cfg [--load_unique_password | --
load_default_password]] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c LoadDefaultBmcCfg --
clear_user_cfg --load_default_password
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

6.5.9 Acquiring the BMC System Lockdown Mode Status

Use the "GetLockdownMode" command to execute SUM to get the current BMC system lockdown mode status of the managed systems.

Syntax for Getting the BMC System Lockdown Mode Status of Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c GetLockdownMode
```

Syntax for Getting the BMC System Lockdown Mode Status of Multiple Systems Remote In-Band :

```
sum -I Remote_INB -l <system list file> -c GetLockdownMode [--remote_sum <remote
sum path>]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetLockdownMode
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l SList.txt -c GetLockdownMode
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

6.5.10 Setting the BMC System Lockdown Mode

Use the “SetLockdownMode” command 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 “BmcRotManage” command to manage RoT functions. For details, see *5.4.11 Managing BMC RoT Functions (Single System)*.

Managing RoT Functions on Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c BmcRotManage --action
<action> [--file <evidence.bin.gz>] [--overwrite]
```

Managing RoT Functions on Multiple Systems through Remote In-Band:

```
sum -I Remote_RHI -l <system list file> -c BmcRotManage --action <action> [--
file <evidence.bin.gz>] [--overwrite] [--remote_sum <remote sum path>]
```

Example:

```
Multiple Systems OOB:
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c BmcRotManage --action
UpdateGolden
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c BmcRotManage --action
UpdateGolden
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

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 for Setting the BMC Reset Counters on Multiple Systems through OOB:

```
sum -l <system list file> [-u <username> -p <password>] -c Attestation --action
<action> [--file <filename>] [--overwrite]
```

Syntax for Setting the BMC Reset Counters on Multiple Systems through Remote In-Band:

```
sum -I Remote_RHI -l <system list file> -c Attestation --action <action> [--file
<filename>] [--overwrite] [--remote_sum <remote sum path>]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c Attestation --action Dump
--file measurement.bin --overwrite
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SUM_HOME]# ./sum -I Remote_RHI -l SList.txt -c Attestation --action Dump --file
measurement.bin --overwrite
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD
```

6.5.13 Managing Remote Attestation

As a security mechanism, remote attestation provides a digital signature and allows users to Use the "Attestation" command to manage measurement files on the managed systems as well as and local measurement files with confidence. For details, see *5.4.14 Managing Remote Attestation*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c Attestation --action
<action> [--file <filename>] [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c Attestation --action Dump
--file measurement.bin --overwrite
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.5.14 Getting BMC LAN Settings

Use the “GetBmcLANCfg” command to get the current BMC LAN settings from the managed systems and save them in separate files for each managed system enumerated in the system list file. For details on the “GetBmcLANCfg” command, see the usage notes in *5.4.15 Getting BMC LAN Settings*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBmcLANCfg --file <
BMCLANCfg.xml > [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBmcLANCfg --file
BMCLANCfg.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 saved in an output file, e.g., BMCLANCfg.xml.192.168.34.56. The --overwrite option is used to overwrite the existing file, e.g., BMCLANCfg.xml.192.168.34.56.

6.5.15 Updating BMC LAN Settings

1. Select one managed system as the golden sample for current BMC LAN settings.
2. Follow the steps in *5.4.15 Getting BMC LAN Settings* for the managed system.
3. Edit the configurable element values in the BMC LAN configuration text file BMCLANCfg.xml to the desired values as illustrated in *4.13 BMC LAN Configuration XML File Format*.
4. Set the 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 "ChangeBmcLANCfg" command with the modified BMCLANCfg.xml file to update the BMC LAN configurations for multiple systems.
7. The IPv4 settings *IPAddr, SubNetmask, DefaultGateWayAddr* in the IPv4 table cannot be applied to each managed system.
8. Use the --individually option to update each managed system with the corresponding configuration file.

Note: For details on the "ChangeBmcLANCfg" command, see the usage notes in *5.4.16 Updating BMC LAN Settings.*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeBmcLANCfg --
file <BMCLANCfg.xml> [--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcLANCfg --file
BMCLANCfg.xml

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcLANCfg --file
BMCLANCfg.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 LAN settings are updated.

If you want to update 192.168.34.56 and 192.168.34.57 with the corresponding configuration file, you need to provide two files: BMCLANCfg.xml.192.168.34.56 and BMCLANCfg.xml.192.168.34.57. Then set the --file argument with the BMCLANCfg.xml file name. With the --individually option, SUM searches for BMCCfg.xml.192.168.34.56 and BMCLANCfg.xml.192.168.34.57 to update 192.168.34.56 and 192.168.34.57, respectively.

6.5.16 Getting the BMC User List

Use the “GetBmcUserList” command to get the current BMC user list from multiple managed systems. For details, see *5.4.17 Get BMC User List*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBmcUserList
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBmcUserList

SList.txt:

    192.168.34.56

    192.168.34.57
```

```
If the execution “Status” field for a managed system is SUCCESS, get the list of
BMC users of the managed system.
```

6.5.17 Setting the BMC User List

Use the “SetBmcUserList” command to set the current BMC user list from multiple managed systems. For details, see *5.4.18 Set BMC User List*.

Note: "No Access,” a user privilege, is not supported on platforms later than X11/H11.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c SetBmcUserList --
action <action> [--user_id <userid> --user_name <username> --user_password
<userpassword> --user_privilege <userprivilege>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --action
add --user_id 3 --user_name ADMIN123 --user_password ADMIn123 --user_privilege 4

SList.txt:

    192.168.34.56

    192.168.34.57

If the execution “Status” field for a managed system is SUCCESS, its BMC user
lists are set.
```

6.5.18 Managing the RMCP Service Port

Use the “RmcpManage” command to get RMCP information and manage RMCP service port. For details, see *5.4.20 Managing RMCP Service Port*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c RmcpManage --action
<GetInfo|Enable|Disable> [--port <port>]
```

```
Example:

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p ADMIN -c RmcpManage --action

Enable --port RMCP:623

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p ADMIN -c RmcpManage --action

Enable --port 623

SList.txt:

    192.168.34.56

    192.168.34.57
```

6.6 Event Log Management for Multiple Systems

6.6.1 Getting the System Event Log

Use the “GetEventLog” command 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 the --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] [--raw_data] [--no_banner]
```

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 --overwrite option is used to force overwrite of the existing file, e.g., EventLog.txt.192.168.34.56. If the --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 “ClearEventLog” command 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 [[--
current_password <current password>] | [--cur_pw_file <current password file
path>]] [--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 “GetMaintenEventLog” command to have SUM show the managed system’s current maintenance event logs (including both BIOS and BMC event logs) and use the --file option to save them in the output files separately. Without the --file option, 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).*

 5.5.3 Getting System

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetMaintenEventLog [-
-st <start time> --et <end time>] [--count <log count>]  [--file <
MaintenEventLog.txt> [--overwrite]]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetMaintenEventLog --st
20200601 --et 20200602 --count 5 --file MaintenEventLog.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 --overwrite option is used to force to overwrite the existing file, e.g., MaintenanceEventLog.txt.192.168.34.56. If the --file option 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 “GetHostDump” command 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 “ClearMaintenEventLog” command 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 Getting CMM Image Information

Use the "GetCmmInfo" command to get 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
Supermicro_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 "UpdateCmm" command with the CMM firmware image Supermicro_CMM.rom to update the 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
Supermicro_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 Getting CMM Settings

Use the "GetCmmCfg" command 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 Getting CMM Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetCmmCfg --file <
CmmCfg.xml > [--overwrite]

sum -l <system list file> -u <username> -p <password> -c GetCmmCfg --file <
CmmCfg.xml> [--overwrite] [--download [--profile_repo]]
```

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 --overwrite option is used to force the overwrite of the existing file, e.g., CMMCfg.xml.192.168.34.56.

Note: For details on profile updates, please refer to *6.16 Profile Update for Multiple Blade Systems*.

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 Getting 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 "ChangeCmmCfg" command 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)*.
- For details on profile update, please refer to *6.16 Profile Update for Multiple Blade*

Systems.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeCmmCfg --file
<CMMCfg.xml> [--individually]
```

```
sum -i <system list file> [-u <username> -p <password>] -c ChangeCmmCfg {[--
upload --file <CmmCfg.xml>] | [--update Apply|Deploy]}
```

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.
In the example, 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, and then Then name the --file argument as “CMMCfg.xml.” 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 “SetCmmPassword” command 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 “LoadDefaultCmmCfg” command 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 Getting BBP Image Information

Use the “GetBbpInfo” command to get 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 Getting 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 “UpdateBbp” command 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 “GetBladePowerStatus” command 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 “SetBladePowerAction” command 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 5 = softshutdown 24 = accycle
--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.

6.7.11 Managing Profile Information

Use the “ProfileManage” command to manage profile information on the CMM. The information will be the same as that in 5.6.7 Managing profile Information (Single System).

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ProfileManage --
action <action> [--file <filename>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ProfileManage --action
Get --file Profile.xml
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the Status field for a managed system shows “SUCCESS,” the profile information of the managed system will be shown in the “Execution Message” section in the created log file.

6.7.12 Receiving Switch Firmware Image Information

Use the "GetSwitchInfo" command to get the switch firmware image information as well as the local switch firmware image (with the --file option) from the managed system. For details, see *5.6.12 Receiving Switch Firmware Image Information (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetSwitchInfo [--
dev_id <Device ID>] [--file <filename>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetSwitchInfo
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetSwitchInfo --dev_id
A1,A2 --file Supermicro_Switch.bin
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.7.13 Updating the Switch Firmware

Use the “UpdateSwitch” command with the Supermicro_Switch.bin switch firmware image to update the managed switch. The information is the same as that in *5.6.13 Updating the Switch Firmware.*

Syntax:

```
sum -l <switch list file> [-u <Switch username> -p <Switch password>] -c
UpdateSwitch --file <filename> [--reboot] [--individually]
```

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateSwitch --file
<filename> [--dev_id <Switch device ID> --switch_user <Switch username> --
switch_pw <Switch password>] [--reboot] [--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SwitchList.txt -u ADMIN -p PASSWORD -c UpdateSwitch --file
Supermicro_Switch.bin --reboot
```

```
[SUM_HOME]# ./sum -l SwitchList.txt -u ADMIN -p PASSWORD -c UpdateSwitch --file
Supermicro_Switch.bin --reboot --individually
```

```
SwitchList.txt:
    192.168.34.100
    192.168.34.101
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateSwitch --file
Supermicro_Switch.bin --dev_id A1 --switch_user ADMIN --switch_pw ADMIN --reboot
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateSwitch --file
Supermicro_Switch.bin --dev_id A1 --switch_user ADMIN --switch_pw ADMIN --reboot
--individually
```

```
SList.txt:
    192.168.34.100
    192.168.34.101
```

For --inidividually option usage, if you want to update 192.168.34.100 and 192.168.34.101, you need to provide two files Supermicro_Switch.bin.192.168.34.100 and Supermicro_Switch.bin.192.168.34.101. Then set the --file argument with the “Supermicro_Switch.bin” filename. With the --individually option, SUM searches for Supermicro_Switch.bin.192.168.34.100 and Supermicro_Switch.bin.192.168.34.100 to update 192.168.34.100 and 192.168.34.101 respectively.

6.7.14 Rebooting the Switch

Use the "RebootSwitch" command to reboot the managed switch. The information will be the same as that in *5.6.14 Rebooting the Switch*.

Syntax:

```
sum -l <switch list file> [-u <Switch username> -p <Switch password>] -c
RebootSwitch
```

```
sum -l <system list file> [-u <username> -p <password>] -c RebootSwitch [--
dev_id <Switch device ID> --switch_user <Switch username> --switch_pw <Switch
password>]
```

Example:

```
[SUM_HOME]# ./sum -l SwitchList.txt -u ADMIN -p PASSWORD -c RebootSwitch
```

```
SwitchList.txt:
    192.168.34.100
    192.168.34.101
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c RebootSwitch --dev_id A1
--switch_user ADMIN --switch_pw ADMIN
```

```
SList.txt:
    192.168.34.100
    192.168.34.101
```

6.8 Applications for Multiple Systems

6.8.1 Sending an IPMI Raw Command

Use the “RawCommand” command 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.

6.8.2 Controlling the UIDs of Multiple Managed Systems

Use the “LocateServerUid” command 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.

6.8.3 Booting into the ISO Image from HTTP Server

Use the "SetHttpBoot" command 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 [[--
current_password <current password>] | [--cur_pw_file <current password file
path>]] [--boot_lan <boot lan port>] [--boot_name <boot description>] --
image_url <URL> [--reboot] --file <file name>
```

```
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_name
bootDescription --image_url http://192.168.12.78/iso/efishell.iso --reboot
```

```
[SUM_HOME]# ./sum -i SList.txt -u ADMIN -p PASSWORD -c SetHttpBoot --boot_lan 2
--boot_name bootDescription --file TLS.crt --image_url
https://[1234:ab5:0:c678:9012:345d:6e78:9f0a]/iso/efishell.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.
- 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 the HTTP boot option.
- When you execute the SetHttpBoot command on the FreeBSD 12 system, you may boot into FreeBSD instead of efishell.iso because of startup.nsh in the system. To prevent from it, you can delete startup.nsh or rename the file name.

6.8.4 Managing KMS Server Configurations

Use the “KmsManage” command to change the KMS server configurations, upload TLS certificates and test the connection to the KMS server. The command is only available on X12/H12 and later platforms. For details on the console output and command usage, see 5.7.11 Managing KMS Server Configurations (Single System).

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c KmsManage
[[--current_password <current password>] | [--cur_pw_file <current password
filename>]]
[option …]
```

Option	Augument	Descriptions
--server_ip	<server IP address>	Enters a KMS server IP address.
--second_server_ip	<second server IP>	Enters a second KMS server IP address.
--port	<port>	Command optional port(s). The format of <port> is “TCP:5696” or “5696”. TCP is for KMS server port.
--time_out	<time out>	Enters a KMS server connection time-out.
--time_zone	<time zone>	Enters a correct time zone.
--client_username	<client username>	Enters a client identity: UserName.
--client_password	<client password>	Enters a client identity: Password.
--ca_cert	<CA certificate filename>	Uploads a CA certificate from the file.
--client_cert	<client certificate filename>	Uploads a client certificate from the file.
--pvt_key	<client private key>	Uploads a client private key from the file.
--pvt_key_pw	<private key password>	Uploads a client private key from the file.
--file	<file name>	When the --action GetInfo option is specified, save the OEM configuration to a file. Otherwise, update the OEM settings with the given configuration file.
--action	<action>	Sets the KMS management action to: 1 = GetInfo: Check the current KMS configurations. 2 = Probe: Test the connection to the specified KMS server. 3 = DeleteCA: Delete a CA certificate. 4 = DeleteCert: Delete a client certificate. 5 = DeletePvtKey: Delete a client private key.

Option	Augument	Descriptions
		6 = DeleteAll: Delete all certificates and keys.
--reboot	N/A	Forces the managed system to reboot or power up after operation.
--post_complete	N/A	Waits for the managed system POST to complete after reboot.

```
Example:

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c KmsManage --server_ip
192.168.12.78 --port 5659 --ca_cert ca.crt --client_cert client.crt --pvt_key
private.key --action Probe --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c KmsManage --server_ip
192.168.12.78 --port TCP:5659 --ca_cert ca.crt --client_cert client.crt --
pvt_key private.key --action Probe --reboot

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c KmsManage --action
GetInfo

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c KmsManage --action
DeleteAll --reboot

SList.txt:
    192.168.34.56
    192.168.34.57
```

If the “Status” field for a managed system shows 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.

6.8.5 Getting System Settings

Use the “GetSystemCfg” command to get the current system settings from the managed systems and save them in the output files individually for each managed system enumerated in the system list file. For details on the “GetSystemCfg” command, see the notes in 5.7.12 Getting System Settings.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetSystemCfg --file
<SystemCfg.xml> [--overwrite] [[--download] [--file_id]]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetSystemCfg --file
SystemCfg.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., SystemCfg.xml.192.168.34.56. The --overwrite option is used to force an existing file to be overwritten , e.g., SystemCfg.xml.192.168.34.56.

Note: For details on profile update, please refer to *6.16 Profile Update for Multiple Blade Systems*.

6.8.6 Updating System Settings

1. Follow the steps in 5.7.13 Updating System Settings.
2. Use the "ChangeSystemCfg" command with the modified SystemCfg.xml file to update the system configurations for multiple systems.

Notes:

- For BMC configuration, 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 BMC configuration file.
- For more details, please refer to 5.3.4 Updating BIOS Settings Based on the Current BIOS Settings and 5.4.4 Updating BMC Settings.
- Use the --individually option to update each managed system with the corresponding configuration file concurrently.
- For details on the "ChangeSystemCfg" command, see the notes in 5.7.13 Updating System Settings.
- For details on profile update, please refer to 6.16 Profile Update for Multiple Blade Systems.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeSystemCfg --
file <SystemCfg.xml> [--reboot [--post_complete]]

sum -l <system list file> [-u <username> -p <password>] -c ChangeSystemCfg {[--
update Apply|Deploy --dev_id <Device ID> --file_id <file ID> --reboot] | [--
upload --file SystemCfg.xml]}
```

Example:

```
[SUM_HOME]# ./sum -l <system list file> [-u <username> -p <password>] -c
ChangeSystemCfg --file SystemCfg.xml

[SUM_HOME]# ./sum -l <system list file> [-u <username> -p <password>] -c
ChangeSystemCfg --file SystemCfg.xml --individually

[SUM_HOME]#./sum -l <system list file> [-u <username> -p <password>] -c
ChangeSystemCfg --upload --file SystemCfg.xml
```

```
[SUM_HOME]# ./sum -l <system list file> [-u <username> -p <password>] -c
ChangeSystemCfg --update Apply --dev_id A1_1,B11_2,A10 --file_id 2 --reboot
```

```
[SUM_HOME]# ./sum -l <system list file> [-u <username> -p <password>] -c
ChangeSystemCfg --update Apply --dev_id ALL --file_id 2 --reboot
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the Status field of a managed system shows “SUCCESS”, its system settings are updated.

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files SystemCfg.xml.192.168.34.56 and SystemCfg.xml.192.168.34.57, and then rename the --file argument as “SystemCfg.xml.” With the --individually option, SUM searches for SystemCfg.xml.192.168.34.56 and SystemCfg.xml.192.168.34.57 to update 192.168.34.56 and 192.168.34.57 respectively.

6.8.7 Invoking Redfish API

Use the “RedfishApi” command to invoke any Redfish API and display the response on screen. For details, please see *5.7.14 Invoke Redfish API*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c RedfishApi --api <api
path> [-v] [--request <http method>] [--file <file name> [--overwrite]] [--data
<request body>] [--retry <number>][--individually]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c RedfishApi  --request
PATCH --api /redfish/v1/TaskService -v --retry 1 --data @body.txt --file
response.txt --overwrite --individually
```

```
SList.txt:
    192.168.34.56

    192.168.34.57
```

If you want to invoke a Redfish API to 192.168.34.56 and 192.168.34.57, and you want them to use different request body, you need to provide two files body.txt.192.168.34.56 and body.txt.192.168.34.57, and then specify --data argument as “@body.txt.” With the --individually option, SUM searches for body.txt.192.168.34.56 and body.txt.192.168.34.57 as the request body sending to 192.168.34.56 and 192.168.34.57 respectively.

6.8.8 Remote Execution

Use the "RemoteExec" command to secure copy the file and execute shell commands on remote Linux systems. For details, see *5.7.15 Remote Execute(Single System)*.

Syntax:

```
sum -I Remote_INB -l Slist.txt -c RemoteExec --remote_cmd <shell command> [--
file <file name>]
```

The managed systems should be enumerated row by row in the system list file. For the "RemoteExec" command, three formats are supported. The system list file should be like this:

```
   Format 1: OS_IP_or_HostName

   Format 2: OS_IP_or_HostName OS_Username OS_Password

   Format 3: OS_IP_or_HostName OS_Username OS_Privatekey OS_Privatekey_Password
```

Use any of the formats when one of these conditions occurs:

- **Format 1 Slist.txt**:

  a). Hosts by different names or IP addresses share the same OS username and password.

  b). Hosts by different names or IP addresses share the same OS password, privatekey, and privatekey password.

- **Format 2 Slist.txt**: Each host has its OS username and password.
- **Format 3 Slist.txt**: Each host has its own OS username, privatekey, and privatekey password.

Example:

Remote In-Band:

```
[SUM_HOME]# ./sum -I Remote_INB -l Slist.txt -c RemoteExec --remote_cmd "ls
/tmp/ -l | grep test.sh" --file test.sh
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

```
[SUM_HOME]# ./sum -I Remote_INB -l Slist.txt -c RemoteExec --remote_cmd "ls
/tmp/ -l | grep test.sh" --file test.sh
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

```
[SUM_HOME]# ./sum -I Remote_INB -l Slist.txt -c RemoteExec --remote_cmd "ls
/tmp/ -l | grep test.sh" --file test.sh
```

```
SList.txt:
    192.168.34.56 root 111111
    192.168.34.57 root 111111
```

```
[SUM_HOME]# ./sum -I Remote_INB -l Slist.txt -c RemoteExec --remote_cmd "ls
/tmp/ -l | grep test.sh" --file test.sh
```

```
SList.txt:
    192.168.34.56 privatekey1 privatekey1_password
    192.168.34.57 privatekey2 privatekey2_password
```

If the execution “Status” field of the managed system shows 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:

- The file will be copied to the path "/tmp/" in remote Linux systems.
- The stderr on the remote Linux system will be redirected to stdout.

6.9 Storage Management for Multiple Systems

6.9.1 Getting RAID Firmware Image Information

Use the “GetRaidControllerInfo” command to get 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 “UpdateRaidController” command 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 Supermicro_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 Getting RAID Settings

Use the “GetRaidCfg” command 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 Getting 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 --overwrite option 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 Getting 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 "ChangeRaidCfg" command 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, and then rename the --file argument as “RAIDCfg.xml.” 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 “GetSataInfo” command to get 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 "GetNvmeInfo" command to get 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 “SecureEraseDisk” command 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> [[--current_password <current password>] | [--cur_pw_file
<current password file path>]] [--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 “SecureEraseRaidHdd” command 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 “SecureEraseRaidHdd” command appended with the --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 “GetPMemInfo” command to get 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 “UpdatePMem” command 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]] [[--current_password <current password>] |
[--cur_pw_file <current password file path>]] [--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.

6.9.11 Getting VROC Settings

Use the "GetVROCCfg" command to get the current VROC settings from the managed systems and save them separately for each managed system enumerated in the system list file. For details on using the "GetVROCCfg" command, see the usage notes in *5.8.11 Getting VROC Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetVROCCfg --file <
VROC.cfg.xml> [--overwrite]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetVROCCfg --file
VROC.cfg.xml --overwrite
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the "Status" field for a managed system (e.g., 192.168.34.56) shows SUCCESS, its current settings are stored in its output file, e.g., VROC.cfg.xml.192.168.34.56. The --overwrite option is used to force the overwrite of the existing file, e.g., VROC.cfg.xml.192.168.34.56.

6.9.12 Updating VROC Settings

1. Follow the steps in *6.9.11 Getting VROC Settings*.
2. Edit the configurable element values in the VROC configuration xml file VROC.cfg.xml as illustrated in *4.11 Format of the VROC Configuration XML File*.
3. Set Action attribute as "None" to skip the unchanged tables in the XML file. Note that this step is optional.
4. Remove the unchanged tables/elements in the XML file. Note that this step is optional.
5. Use the "ChangeVROCCfg" command with the modified VROC.cfg.xml file to update the VROC configurations for multiple systems.

Notes:

- Use the --individually option to update each managed system with the corresponding configuration file concurrently. The --individually option is required for this command.
- For details on the "ChangeVROCCfg" command, see the usage notes in *5.8.12 Updating VROC Settings (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeVROCCfg --file
<VROC.cfg.xml> --individually
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeVROCCfg --file
VROC.cfg.xml --individually

SList.txt:
    192.168.34.56

    192.168.34.57
```

If the "Status" field for a managed system is SUCCESS, its VROC settings are updated.

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files VROC.cfg.xml.192.168.34.56 and VROC.cfg.xml.192.168.34.57, and then rename the --file argument as

“VROC.cfg.xml.” With the --individually option, SUM searches for VROC.cfg.xml.192.168.34.56 and VROC.cfg.xml.192.168.34.57 to update 192.168.34.56 and 192.168.34.57 respectively.

6.9.13 Control NVMe Device

Use the "ControlNvme" command to locate, insert or remove NVMe devices. The information will be the same as that in *6.9.6 Getting NVMe Information (Single System)*.

Syntax:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ControlNvme --action
<Action> --dev_id <device ID> --group_id <group ID> --slot <slot num>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ControlNvme --action
Locate --dev_id 0 --group_id 0 --slot 0
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

6.10 NIC Management for Multiple Systems

6.10.1 Getting Add-On NIC Firmware Image Information

Use the “GetAocNICInfo” command to get the add-on NIC firmware information from the managed system as well as the add-on NIC local firmware image. The information will be the same as that in *5.9.1 Getting Add-On NIC Firmware Image Information (Single System).*

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetAocNICInfo [--file
<filename>] [--dev_id <add-on NIC device ID >]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetAocNICInfo  --file
AOC_NIC.bin
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the “Status” field for a managed system is SUCCESS, the add-on NIC 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 Add-On NIC Firmware Image

Use the “UpdateAocNIC” command with the add-on NIC firmware image AOC_NIC.bin to update the managed system. For details, please see the usage notes in 5.9.2 Updating the Add-On NIC Firmware Image (Single System).

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateAocNIC --file
<filename> --dev_id <add-on NIC device ID> --reboot [--post_complete]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateAocNIC --file
AOC_NIC.bin --dev_id 1 --reboot --post_complete
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

The execution results for the managed system will be the most updated in the “Execution Message” section of the managed system in the created log file.

6.11 PSU Management for Multiple Systems

6.11.1 Getting PSU Information

Use the "GetPsuInfo" command 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.

6.11.2 Updating the Signed PSU Firmware Image Requested by OEM

Use the "UpdatePsu" command 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
Supermicro_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.

6.11.3 Getting the Current Power Status of the Managed System

Use the “GetPowerStatus” command 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.

6.11.4 Setting Power Action of Managed System

Use the “SetPowerAction” command 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.

6.12 TPM Management for Multiple Systems

6.12.1 Getting TPM Information

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the "GetTpmInfo" command to get the TPM module information from the managed system. For details on 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.

6.12.2 Provisioning the TPM Module

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the "TpmManage" command 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 details on 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 "TpmProvision" command 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.

6.12.3 Enabling and Clearing TPM Module Capabilities

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the "TpmManage" command with the options in the following table to provide TPM module capabilities from the managed system. For detailes, 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 “TpmProvision” command with options “--cleartpm and” --reboot to clear TPM module capabilities from managed systems. For details on the “--cleartpm” option, 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.

6.13 GPU Management for Multiple Systems

6.13.1 Getting GPU Information

Use the "GetGpuInfo" command to get the current GPU information from the managed systems. The GPU information output will be the same as that in *5.12.1 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 GPU information of the managed system will be shown in the "Execution Message" section of the managed system in the created log file.

6.13.2 Updating the GPU Firmware Image

Use the “UpdateGpu” command with CEC/FPGA of GPU firmware image to run SUM to update the GPU firmware of a managed system. For details, please see the usage notes in *5.12.2 Updating the GPU Firmware Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateGpu --item
<CEC|FPGA> --file <filename>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateGpu --item FPGA --
file GPU_FPGA.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.

6.14 CPLD Management for Multiple Systems

6.14.1 Getting CPLD Firmware Image Information (Multiple Systems)

Use the “GetCpldInfo” command to get 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 “UpdateCpld” command 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.

6.15 AIP Management for Multiple Systems

6.15.1 Getting AIP CPLD Information

Use the “GetAipCpldInfo” command to get the current AIP CPLD information from the managed systems installed with AIP. The AIP CPLD information output will be the same as that in *5.14.1 Getting AIP CPLD Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetAipCpldInfo
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetAipCpldInfo
```

```
SList.txt:
    192.168.34.56
    192.168.34.57
```

If the “Status” field of a managed system is SUCCESS, the AIP CPLD information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.15.2 Updating the AIP CPLD Firmware Image

Use the “UpdateAipCpld” command with a given AIP CPLD firmware image to run SUM to update the AIP CPLD firmware of a managed system with AIP installed. For details, see the notes in *5.14.2 Updating the AIP CPLD Firmware Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateAipCpld --file
<filename>
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateAipCpld --file
AIP_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.

6.16 Profile Update for Multiple Blade Systems

SUM supports profile update for multiple Blade systems. profile update is only supported on the Blade system with 64MB CMM AST2400. You can use the ChangeCmmCfg/ChangeSystemCfg commands with the --upload option to manage the CMM and Blade configurations of multiple Blade systems, upload one CMM profile and up to twenty system profiles, and upload CMM/Blade system configurations to CMMwith. Use the ProfileManage command to edit and get the existing profile information from CMM. Note that there is a space limit on Profiles. Once the space is full, use the ProfileManage command to delete unnecessary profiles, and upload new profiles. Each profile name on CMM is unique. Different profiles with the same profile names cannot exist on CMM at the same time. For more details about the usages of profile update and update rules, see *5.14 Profile Update for a Single Blade System*.

6.16.1 Profile Management (Multiple Systems)

SUM supports profile management for multiple Blade systems. For more details, see *5.14.2 Profile Management*.

6.16.2 Updating CMM Configurations (Multiple Systems)

SUM supports updating CMM configurations for multiple Blade systems through the existing CMM profiles on CMM. For more details, see *5.14.3 Updating CMM Configurations*.

6.16.3 Updating System Configurations (Multiple Systems)

SUM supports updating system configurations for multiple Blade systems through the existing system profiles on the CMM. For more details, see *5.14.4 Update Blade configurations*.

6.17 TwinPro Management for Multiple Systems

6.17.1 Getting TwinPro Settings

Use the “GetBmcCfg” command to get the current BMC settings from the managed systems and save them in output files individually for each managed system enumerated in the system list file. For details on the “GetBmcCfg” command, see the usage notes in *5.17.1 Getting TwinPro Settings (Single System)*.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetTpCfg --file <
TpCfg.xml > [--overwrite]
```

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetTpCfg --file TpCfg.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., TpCfg.xml.192.168.34.56. The --overwrite option is used to force overwrite the existing file, e.g., TpCfg.xml.192.168.34.56.

6.17.2 Updating TwinPro Settings

1. Select one managed system as the golden sample for current BMC settings.
2. Follow the steps in *5.17.1 Getting TwinPro Settings* for the managed system.
3. Edit the configurable element values in “BMCCfg.xml,” a BMC configuration text file, to the desired values as illustrated in *4.9 Format of TwinPro 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 “ChangeTpCfg” command with the modified TpCfg.xml file to update the BMC configurations for multiple systems.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c ChangeTpCfg --file <
TpCfg.xml> [--individually]

Example:

Multiple Systems OOB:

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeTpCfg --file
TpCfg.xml

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c ChangeTpCfg --file
TpCfg.xml --individually

SList.txt:

    192.168.34.56

    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, its TiwnPro settings are updated.

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files TpCfg.xml.192.168.34.56 and TpCfg.xml.192.168.34.57. Then set the --file argument with the TpCfg.xml file name. With the --individually option, SUM will search for TpCfg.xml.192.168.34.56 and TpCfg.xml.192.168.34.57 to update 192.168.34.56 and 192.168.34.57, respectively.

6.18 CDU Management for Multiple Systems

Use the “MonitorCDUStatus” command to access the function to show or set the current CDU Web UI Status remotley. The message output will be the same as that in 5.18 CDU Management for a Single System.

Multiple Systems OOB Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c MonitorCDUStatus --
action <action> [--file <CDUStatus.txt>] [--overwrite] [--file
<CDU_alert_setting.json file>]
```

Option Commands	Descriptions
--action	Sets CDU action to: 1 = GetStatus 2 = SetCfg

Example:

Multiple Systems OOB:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MonitorCDUStatus --action
GetStatus --file CDUStatus.txt --overwrite

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MonitorCDUStatus --action
SetCfg --file CDU_alert_setting.json

SList.txt:

    192.168.34.56

    192.168.34.57
```

If the execution “Status” field for a managed system is SUCCESS, the CDU status of the managed system will be shown in the “Execution Message” section in the created log file.

6.19 Backplane Management for Multiple Systems

6.19.1 Getting Multi-node EC Firmware Image Information

Use the “GetMultinodeEcInfo” command to get the multi-node EC firmware image information from the managed system as well as the input multi-node EC firmware image. For details, see *5.19.1 Getting Multi-node EC Firmware Image Information* (Single System).

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetMultinodeEcInfo [-
-file <filename>]
```

```
Example:
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetMultinodeEcInfo
```

```
SList.txt:
    192.184.11.65
    192.168.34.57
```

If the execution “Status” field for the managed system is SUCCESS, the multi-node EC firmware image information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

6.19.2 Updating a Multi-node EC Firmware Image

Use the "UpdateMultinodeEc" command with the given multi-node EC firmware image EC.bin to run SUM to update the multi-node EC firmware of managed systems. For details, see the notes in *5.19.2 Updating the Multi-node EC Firmware Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateMultinodeEc --
file <filename>
```

Example:

```
[SUM_HOmE]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateMultinodeEc --file
EC.bin
```

```
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.

Note: This command can only be operated on node A of a system to perform a multi-node EC FW update.

6.19.3 Getting Backplane CPLD Firmware Information

Use the "GetBackplaneCpldInfo" command to get the backplane CPLD firmware image information from the managed system. For details, see *5.19.1 Getting Backplane CPLD Firmware Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetBackplaneCpldInfo
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetBackplaneCpldInfo
```

```
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.

6.19.4 Updating the Backplane CPLD Firmware Image

Use the "UpdateBackplaneCpld" command with the backplane CPLD firmware image to update the backplane CPLD firmware of a managed system. For details, see *5.19.2 Updating Backplane CPLD Firmware Image (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c UpdateBackplaneCpld
<--index <0|1|2|3> --file BPN_CPLD.jed | --update_list
0:BPN_CPLD.jed[,1:Backplane_CPLD.jed]...]> --manual_ejected
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c UpdateBackplaneCpld --
index 0 --file BPN_CPLD.jed --manual_ejected
```

```
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.

6.20 Virtual Media Management for Multiple Systems

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

Use the “MountIsoImage” command to mount an ISO image as virtual media to managed systems through a SAMBA/HTTP/HTTPS server. For details on the “MountIsoImage” command, please refer to *5.19.1 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 MountIsoImag‘ --image_url
'smb://192.168.35.1/MySharedPoint/MyFo’der/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImag‘ --image_url
'smb://[2001:db8::1]/MySharedPoint/MyFo’der/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImag‘ --image_url
'http://192.168.35.1/MySharedPoint/MyFo’der/Image.iso' --id smbid --pw smbpasswd

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImag‘ --image_url
'http://[2001:db8::1]:80/MySharedPoint/MyFo’der/Image.iso' --id smbid --pw
smbpassw

[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImag‘ --image_url
'https://192.168.35.1/MySharedPoint/MyFo’der/Image.iso' --id smbid --pw
smbpasswd
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImag‘ --image_url
'https://[2001:db8::1]:80/MySharedPoint/MyFo’der/Image.iso' --id smbid --pw
smbpassw
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImag‘ --image_url
'\\192.168.35.1\MySharedPoint\MyFo’der\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.

6.20.2 Removing an ISO Image as a Virtual Media

Use the “UnmountIsoImage” command to unmount an ISO image as a virtual media from a 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.

6.20.3 Mounting a Floppy Image Virtually from a Local Image File

Use the “MountFloppyImage” command to execute SUM to mount a binary floppy image virtually to the managed system. For details on “MountFloppyImage,” please refer to *5.19.3 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.

6.20.4 Unmounting a Floppy Image Virtually from the Managed System

Use the “UnmountFloppyImage” command to remove a binary floppy image virtually from the managed system. For details on “UnmountFloppyImage,” please refer to *5.19.4 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.

6.20.5 Getting Virtual Media Information

On the platforms that support multiple virtual media devices, use the “GetVmInfo” command to get the virtual media information from the managed system. For details on the “GetVmInfo” command, please refer to *5.19.5 Get Virtual Media Information (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c GetVmInfo [--dev_id
<device ID>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c GetVmInfo --dev_id 1
```

```
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.

6.20.6 Managing Multiple Virtual Media Devices

For platforms that support multiple virtual media devices, use the “VmManage” command with the Mount/Unmount action to mount or unmount an image. Use the “VmManage” command with the Enable/Disable action to enable or disable virtual media on all platforms. For details on the “VmManage” command, please refer to *5.19.6 Manage Multiple Virtual Media Device (Single System)*.

Syntax:

```
sum -l <system list file> [-u <username> -p <password>] -c VmManage --action
<Enable/Disable> [--port <port>]
```

```
sum -l <system list file> [-u <username> -p <password>] -c VmManage --action
Mount [--dev_id <device ID>] --image_url <URL> [[--id <id for URL> --pw
[password for URL]]|[--id <id for URL> --pwd_file <password file path>]] [--
verify_cert [--accept_self_signed]]
```

```
sum -l <system list file> [-u <username> -p <password>] -c VmManage --action
Unmount [--dev_id <device ID>]
```

Example:

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Enable
--port 623
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Disable
--port 623
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Mount -
-image_url 'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd --dev_id 1
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Mount -
-image_url 'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso' --id smbid --
pw smbpasswd --dev_id 2
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Mount -
-image_url 'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --
pw smbpasswd --dev_id 3
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Mount -
-image_url 'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbid
--pw_file smbpasswd.txt --dev_id 1
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Mount -
-image_url 'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --
pw smbpasswd --verify_cert --accept_self_signed --dev_id 2
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Mount -
-image_url 'https://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id
smbid --pw_file smbpasswd.txt --verify_cert --accept_self_signed --dev_id 3
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Mount -
-image_url '\\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id smbid --
pw_file smbpasswd.txt --dev_id 1
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Mount -
-image_url '\\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id smbid --pw_file
smbpasswd.txt --dev_id 2
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Unmount
--dev_id 1
```

```
[SUM_HOME]# ./sum -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action Unmount
--dev_id ALL
```

```
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 console output of the managed system will be shown in 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 the in-band commands with the --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.**
SystemPFA	**Yes**	**Yes**	Required
MemoryHealthCheck	**Yes**	**Yes**	Required
CpuOnDemand	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
ChassisIntrusion	**Yes**	**Yes**	Not required
GetFruInfo	**Yes**	**Yes**	**Required for --dump option**
RestoreFruInfo	**Yes**	**Yes**	Required
ChangeFruInfo	**Yes**	**Yes**	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 for platforms before X12 Intel® Xeon® E-2300 Series
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	**No**	**Yes**	Not Required
BiosRotManage	**Yes**	**Yes**	**SFT-DCMS-SINGLE is required for Recover and DownloadEvidence actions**
SecureBootManage	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
GetFixedBootCfg	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
ChangeFixedBootCfg	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**

[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)**	
UpdateScp	**Yes**	**No** **(Yes for ARM64)**	Not Required
GetScpInfo	**Yes**	**No** **(Yes for ARM64)**	Not Required
[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 and DownloadEvidence actions.**
TimedBmcReset	**Yes**	**Yes**	Not Required
Attestation	**Yes**	**Yes**	**Both SFT-DCMS-SINGLE and SFT-SDDC-SINGLE are required for action Compare.**
GetBmcUserList	**Yes**	**Yes**	Required
SetBmcUserList	**Yes**	**Yes**	Required
RmcpManage	**Yes**	**Yes**	Required
[System Event Log]			

GetEventLog	**Yes**	**Yes**	Required
ClearEventLog	**Yes**	**Yes**	Required
GetMaintenEventLog	**Yes**	**Yes**	Not Required
GetHostDump	**Yes**	**Yes**	**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
ProfileManage	**Yes**	**No**	Not Required
GetSwitchInfo	**Yes**	**No**	Not Required
UpdateSwitch	**Yes**	**No**	Not Required
RebootSwitch	**Yes**	**No**	Not Required

[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)	
[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**	**Yes**	**Required**
SecureEraseDisk	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
SecureEraseRaidHdd	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
GetPMemInfo	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
UpdatePMem	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
GetVROCCfg	**Yes**	**Yes**	**Required**
ChangeVROCCfg	**Yes**	**Yes**	**Required**
[NIC Management]			
GetAocNICInfo	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
UpdatetAocNIC	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
[Applications]			
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 **SFT-DCMS-SINGLE for TLS upload configuration**
GetSystemCfg	**Yes**	**Yes**	Required
ChangeSystemCfg	**Yes**	**Yes**	Required
RedfishApi	**Yes**	**Yes**	Not Required
RemoteExec	No	**Yes (Remote Only)**	Not Required
[PSU Management]			
GetPsuInfo	**Yes**	**Yes**	Required
UpdatePsu	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
GetPowerStatus	**Yes**	**Yes**	Not Required
SetPowerAction	**Yes**	**Yes**	Not Required

[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)	
[TPM Management]			
TpmProvision	**Yes**	**No**	Required
GetTpmInfo (Supermicro OTA)	**Yes**	**Yes**	Required
GetTpmInfo (Intel OTA)	**Yes**	**Yes**	Required
TpmManage (Supermicro OTA)	**Yes**	**Yes**	Required
TpmManage (Intel OTA)	**Yes**	**Yes**	Required
[GPU Management]			
GetGpuInfo	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
UpdateGpu	**Yes**	**Yes**	**SFT-DCMS-SINGLE only**
[CPLD Management]			
GetCpldInfo	**Yes**	**Yes**	Not Required
UpdateCpld	**Yes**	**Yes**	Not Required
[AIP Management]			
GetAipCpldInfo	**Yes**	**No**	Not Required
UpdateAipCpld	**Yes**	**No**	Not Required
[TwinPro Management]			
GetTpCfg	**Yes**	**Yes**	Required
ChangeTpCfg	**Yes**	**Yes**	Required
[CDU Management]			
MonitorCDUStatus	**Yes**	**No**	Not Required
[Backplane Management]			
GetMultinodeEcInfo	**Yes**	**Yes**	Not Required
UpdateMultinodeEc	**Yes**	**Yes**	Not Required
GetBackplaneCpldInfo	**Yes**	**Yes**	Not Required
UpdateBackplaneCpld	**Yes**	**No**	Not Required
[PCIeSwitch Management]			
GetPCIeSwitchInfo	**No**	**Yes**	Not Required
UpdatePCIeSwitch	**No**	**Yes**	Not Required
[VM Management]			
MountIsoImage	**Yes**	**Yes**	Required
UnmountIsoImage	**Yes**	**Yes**	Required
MountFloppyImage	**Yes**	**Yes**	Required
UnmountFloppyImage	**Yes**	**Yes**	Required
GetVmInfo	**Yes**	**Yes**	Required
VmManage	**Yes**	**Yes**	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

- The 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.
- 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.
- The 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 on 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 either.
- 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 BIOS update through KCS is not supported on an 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 BIOS update 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.
- BIOS updated PMem related configuration, command UpdatePMem with option --restore_default_fw cannot be supported for BIOS after 2022/08/04.
- BIOS updated PMem related configuration, commands GetCurrentBiosCfg, GetDefaultBiosCfg and ChangBiosCfg cannot support PMem related configuration for BIOS after 2022/08/04.

BMC Management

- The UpdateBmc in-band command does not support the AMI BMC firmware image.
- The GetBmcCfg and ChangeBmcCfg in-band commands in Windows do not support a hostname that exceeds 244 bytes.
- The UpdateBmc in-band command on FreeBSD OS will be slow caused by KCS driver of FreeBSD.
- The LAN table in a 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 getting BMC settings may be different. Be careful of not misusing them.

CMM Management (OOB Only)

- All CMM management commands are for OOB use only.

Applications

- When dynamically enabling a USB port with the SetUsbAccessMode command, USB 3.0 devices may need to be manually unplugged and plugged back in to be available.

PSU Management

- The UpdatePsu command only supports PSU “PWS-2K04A-1R” and “PWS-2K20A-1R.”
- The UpdatePsu command does not support multiple OOB usages.

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 the 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.

PCIeSwitch Management

- All PCIeSwitch management commands are for In-Band use only.
- All PCIeSwitch management commands only support H12DGQ-NT6 with Broadcom PCIeSwitch Gen4 Series chipsets and X12DSC-6 with Microchip PCIeSwitch Gen4 Series chipsets platforms.

VM Management

- The function of mounting ISO through IPv6 is not available on H12 AST2500 non-RoT platforms and versions before X12/H12.
- If the device is mounted by iKVM, the device can only be unmounted by iKVM.

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 ChangeBiosCfg command 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 “ChangeBiosCfg” command.

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 “ChangeBiosCfg” command.

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 the 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”) length and maximum length (“MaxSize”). The “AllowingMultipleLine” option 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 the 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 "ChangeBiosCfg"command, SUM will load the file from system and upload it to BIOS. The following example is the setting of TLS upload:

6.20.6.1 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 supported versions and limitations are summarized in the 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

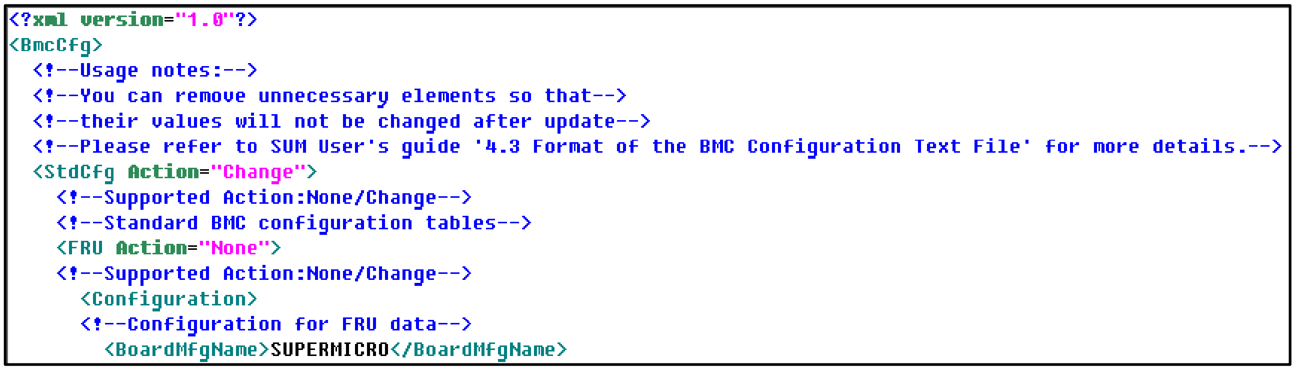
For SUM 2.4.0 and before, none of license SFT-DCMS-SINGLE required BIOS settings can be changed through SUM. Due to known limitation in SUM 2.5.x, even license SFT-DCMS-SINGLE is activated, SFT-DCMS-SINGLE required BIOS settings may not be able to change through SUM. To fully support, please use SUM 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

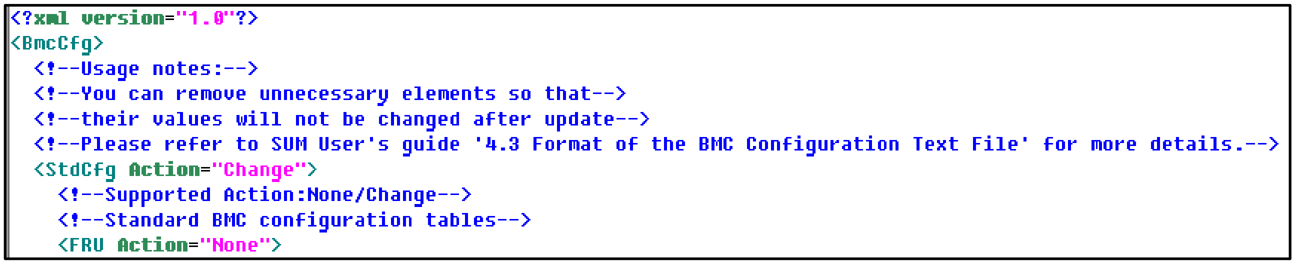
- To set a value (SUPERMICRO) to an element

  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

In this example, Red Hat Enterprise Linux 7 is used 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:

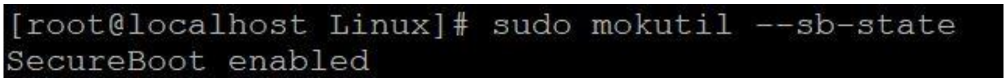
- openSSL
- kernel-devel
- mokutil
- keyutils
- perl (For Kernel version prior to 4.3.3)

2. Check if the option Secure Boot is enabled.

Syntax:

```
[shell]# sudo mokutil --sb-state
```

Example:



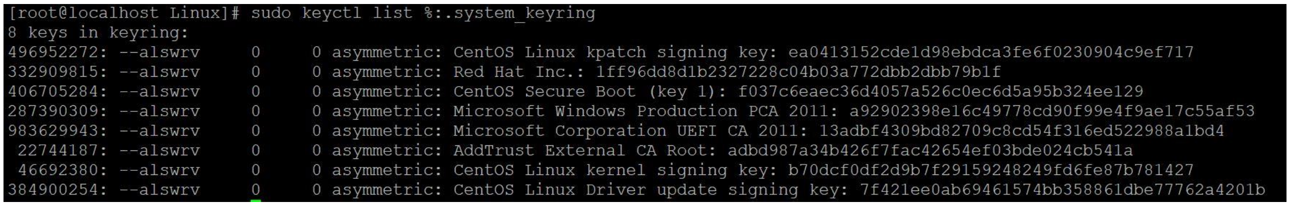
```
[root@localhost Linux]# sudo mokutil --sb-state
SecureBoot enabled
```

3. Check the OS keyring. The SUM output in the example 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.

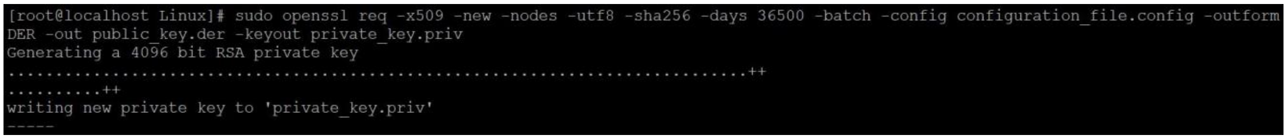
Syntax:

```
[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.

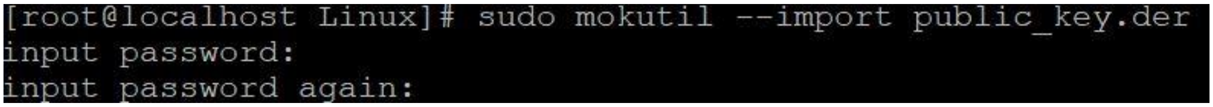
Syntax:

```
[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:

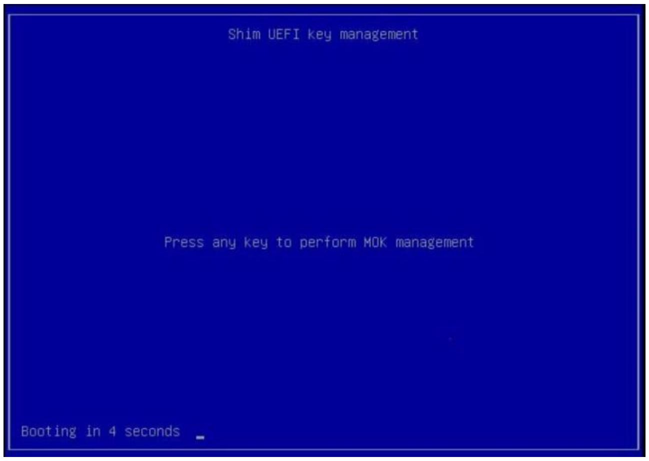


```
[root@localhost Linux]# sudo mokutil --import public_key.der
input password:
input password again:
```

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.

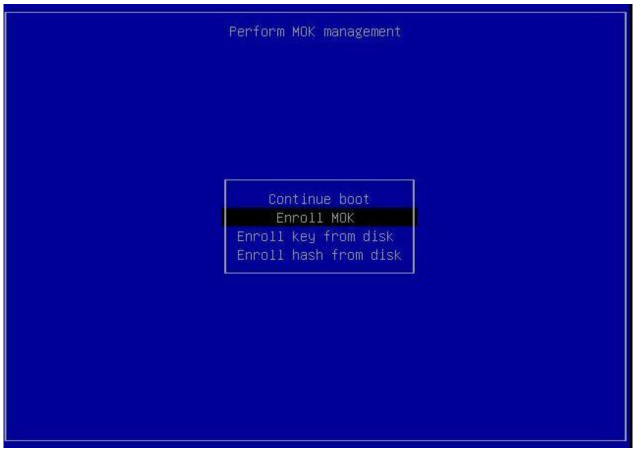


Shim UEFI key management

Press any key to perform MOK management

Booting in 4 seconds _

9. Select **Enroll MOK**.



Perform MOK management

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.

<table>
<tr><td>!</td><td>$</td><td>%</td><td>&</td><td>(</td><td>)</td><td>*</td><td>+</td></tr>
<tr><td>.</td><td>/</td><td><</td><td>=</td><td>></td><td>?</td><td>@</td><td>[</td></tr>
<tr><td>\</td><td>]</td><td>^</td><td>_</td><td>`</td><td>{</td><td>|</td><td>}</td></tr>
<tr><td>~</td><td>-</td><td>:</td><td>,</td><td>;</td><td>#</td></tr>
</table>

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
SystemPFA	No
MemoryHealthCheck	No
CpuOnDemand	No
GetFruInfo	**Yes**
RestoreFruInfo	No
ChangeFruInfo	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**
Attestation	**No**
GetBmcUserList	**Yes**
SetBmcUserList	**No**
RmcpManage	**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**
GetVROCCfg	**Yes**
ChangeVROCCfg	**Yes**

[NIC Management]	
GetAocNICInfo	**Yes**
UpdateAocNIC	**No**
[Applications]	
MountIsoImage	**No**
UnmountIsoImage	**No**
MountFloppyImage	**No**
UnmountFloppyImage	**No**
RawCommand	**Yes**
GetUsbAccessMode	**Yes**
SetUsbAccessMode	**No**
LocateServerUid	**Yes**
SetHttpBoot	**No**
RedfishApi	**Yes**
RemoteExec	**No**
[PSU Management]	
GetPsuInfo	**Yes**
UpdatePsu	**No**
GetPowerStatus	**Yes**
SetPowerAction	**Yes**
[TPM Management]	
TpmProvision	**No**
GetTpmInfo (Supermicro OTA)	**Yes**
GetTpmInfo (Intel OTA)	**Yes**
TpmManage (Supermicro OTA)	**No**
TpmManage (Intel OTA)	**No**
[GPU Management]	
GetGpuInfo	**Yes**
UpdateGpu	**No**
[CPLD Management]	
GetCpldInfo	**Yes**
UpdateCpld	**No**
[AIP Management]	
GetAipCpldInfo	**No**
UpdateAipCpld	**No**
[TwinPro Management]	
GetTpCfg	**Yes**
ChangeTpCfg	**No**
[CDU Management]	
MonitorCDUStatus	**No**
[Backplane Management]	
GetMultinodeEcInfo	**Yes**
UpdateMultinodeEc	**No**

GetBackplaneCpldInfo	**Yes**
UpdateBackplaneCpld	**No**

Appendix K. Using SUM to Run 3rd -Party Tools

To run SUM with a third-party tool on remote systems, execute the RemoteExec command to connect to remote systems. For details on the RemoteExec command, see *5.7.15 Remote Execution*.

K.1 LAN NVM update

Here we use LAN NVM Update Package as the example to guide you through running a third-party tool with SUM.

```
./sum -I Remote_INB --oi <OS_IP> --ou <OS_User> --op <OS_Password> -c
RemoteExec --file "STGF2S3B3_NUP.zip" --remote_Cmd "cd /tmp/ && unzip -o
STGF2S3B3_NUP.zip && cd STGF2S3B3_NUP && chmod +x LLDP_EN.sh && chmod +x
nvmupdate64e && ./LLDP_EN.sh"
```

1. The file STGF2S3B3_NUP.zip on the managing system is copied to the /tmp/STGF2S3B3_NUP.zip path on the remote system.
2. The working directory is changed to /tmp/ to access the files under /tmp/ in a relative path.
3. The “unzip -o STGF2S3B3_NUP.zip” file uncompresses and overwrites the existing files.
4. The working directory is changed to STGF2S3B3_NUP.
5. Both “chmod +x LLDP_EN.sh” and “chmod +x nvmupdate64e” files make the files executable.
6. LLDP_EN(.sh) is an update script from the vendor, nvmupdate64e is the binary to update the firmware, and nvmupdate.cfg is the configuration file required for nvmupdate64e. The “./LLDP_EN.sh” file will call nvmupdate64e with nvmupdate.cfg (relative path in STGF2S3B3_NUP) to update the NIC firmware.

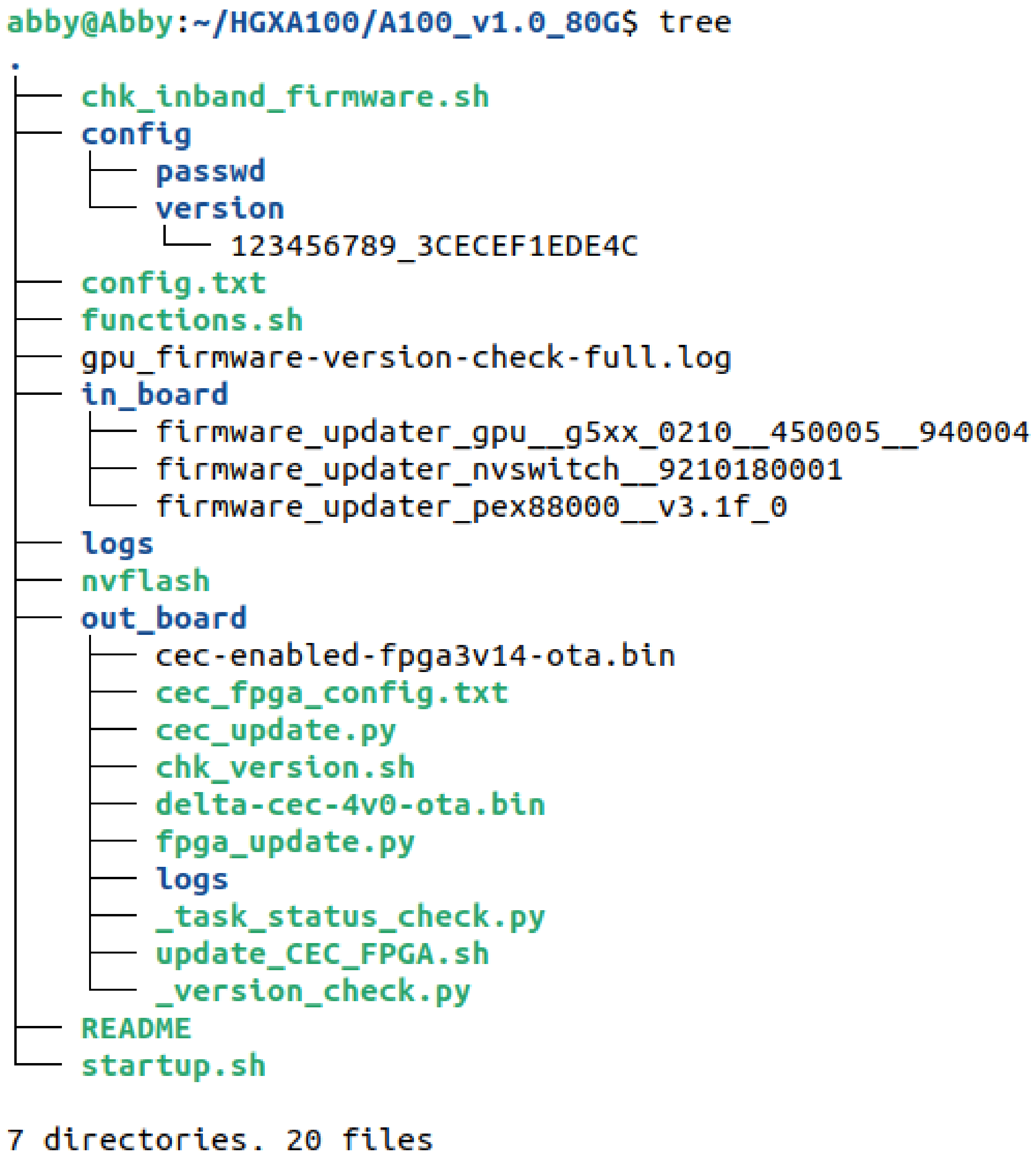
K.2 NVIDIA HGX A100 GPU firmware update package

The main updating GPU firmware package consists of two particular packages; one is script package named as A100_v1.0 and the other is vendor package named as HGX_A100_8-GPU_80G_AC_Firmware_22.05.03.

Both packages are designated for NVIDIA HGX A100 systems with 40 or 80GB memory size GPU firmware updating.

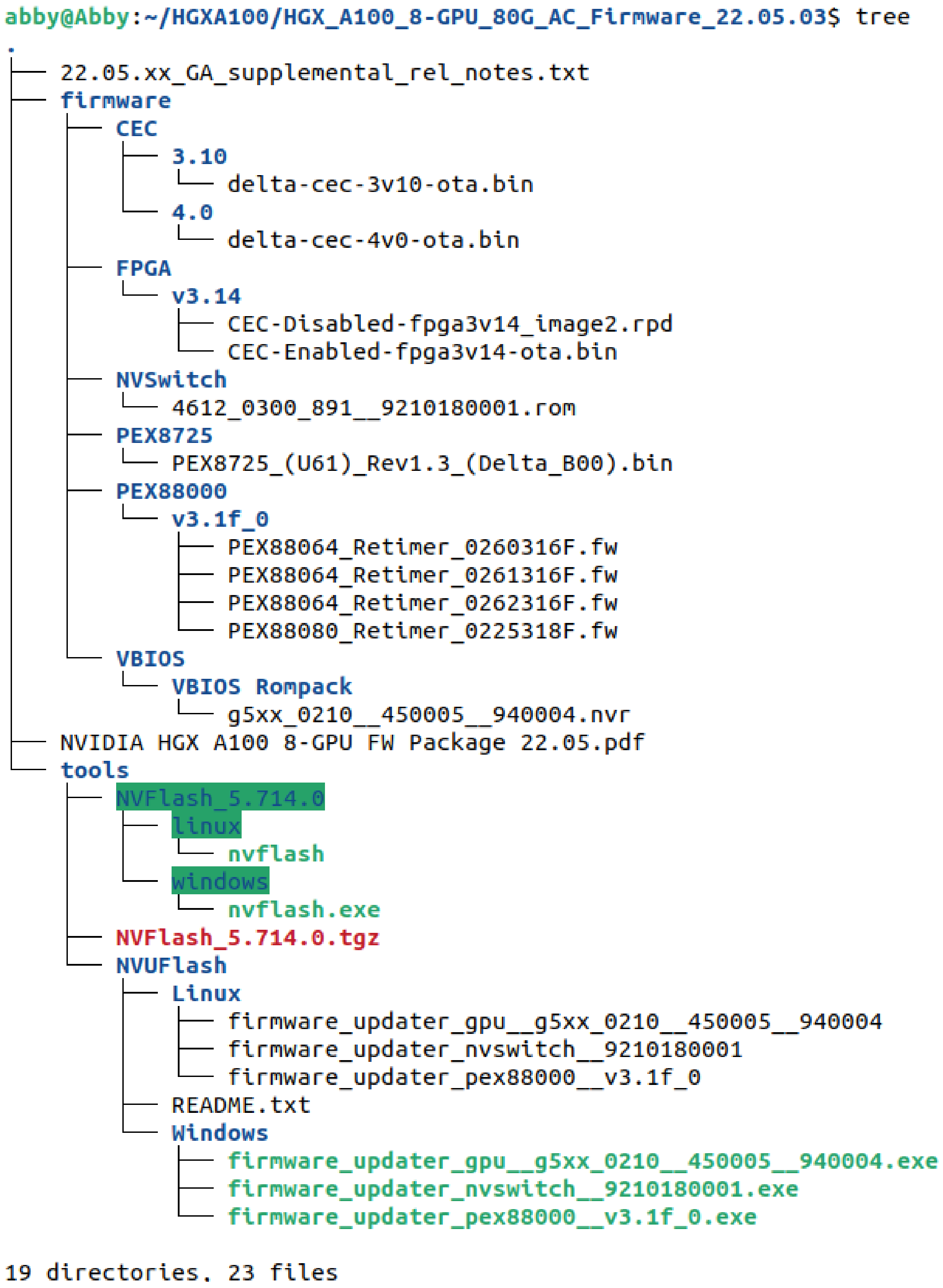
The script package contains scripts and config.txt. SUM would use “startup_INB.sh” and “function.sh” for INB update usage. Also, “startup.sh” would call other NVIDIA tools and firmware version with variables defined in “config_INB.txt”.

Here is the directory tree and list of files in the A100_v1.0.



```
abby@Abby:~/HGXA100/A100_v1.0_80G$ tree
.
├── chk_inband_firmware.sh
├── config
│   ├── passwd
│   └── version
│       └── 123456789_3CECEF1EDE4C
├── config.txt
├── functions.sh
├── gpu_firmware-version-check-full.log
├── in_board
│   ├── firmware_updater_gpu__g5xx_0210__450005__940004
│   ├── firmware_updater_nvswitch__9210180001
│   └── firmware_updater_pex88000__v3.1f_0
├── logs
├── nvflash
├── out_board
│   ├── cec-enabled-fpga3v14-ota.bin
│   ├── cec_fpga_config.txt
│   ├── cec_update.py
│   ├── chk_version.sh
│   ├── delta-cec-4v0-ota.bin
│   ├── fpga_update.py
│   ├── logs
│   ├── _task_status_check.py
│   ├── update_CEC_FPGA.sh
│   └── _version_check.py
├── README
└── startup.sh

7 directories. 20 files
```

The vendor package is provided by NVIDIA. The latest NVIDIA released firmware package version is 22.05.03. Firmware and inband update tools are inside. Here is the directory tree and list of files in the NVIDIA HGX A100 8-GPU Firmware 22.05.03 release package:



```
abby@Abby:~/HGXA100/HGX_A100_8-GPU_80G_AC_Firmware_22.05.03$ tree
.
├── 22.05.xx_GA_supplemental_rel_notes.txt
├── firmware
│   ├── CEC
│   │   ├── 3.10
│   │   │   └── delta-cec-3v10-ota.bin
│   │   └── 4.0
│   │       └── delta-cec-4v0-ota.bin
│   ├── FPGA
│   │   └── v3.14
│   │       ├── CEC-Disabled-fpga3v14_image2.rpd
│   │       └── CEC-Enabled-fpga3v14-ota.bin
│   ├── NVSwitch
│   │   └── 4612_0300_891__9210180001.rom
│   ├── PEX8725
│   │   └── PEX8725_(U61)_Rev1.3_(Delta_B00).bin
│   ├── PEX88000
│   │   └── v3.1f_0
│   │       ├── PEX88064_Retimer_0260316F.fw
│   │       ├── PEX88064_Retimer_0261316F.fw
│   │       ├── PEX88064_Retimer_0262316F.fw
│   │       └── PEX88080_Retimer_0225318F.fw
│   └── VBIOS
│       └── VBIOS Rompack
│           └── g5xx_0210__450005__940004.nvr
├── NVIDIA HGX A100 8-GPU FW Package 22.05.pdf
└── tools
    ├── NVFlash_5.714.0
    │   ├── linux
    │   │   └── nvflash
    │   └── windows
    │       └── nvflash.exe
    ├── NVFlash_5.714.0.tgz
    └── NVUFlash
        ├── Linux
        │   ├── firmware_updater_gpu__g5xx_0210__450005__940004
        │   ├── firmware_updater_nvswitch__9210180001
        │   └── firmware_updater_pex88000__v3.1f_0
        ├── README.txt
        └── Windows
            ├── firmware_updater_gpu__g5xx_0210__450005__940004.exe
            ├── firmware_updater_nvswitch__9210180001.exe
            └── firmware_updater_pex88000__v3.1f_0.exe

19 directories, 23 files
```

The following commands are for INB firmware update for PEX88000, vBIOS and NVSwitch and OOB firmware update for CEC and FPGA. Please refer to “SUM_UpgradeGPU_script.sh” or “SUM_UpgradeGPU_MMscript.sh” script and edit “SUM_Upgrade_cfg.txt” under “SUM folder/script/” to assign remote machine IP/User ID/Password of OS and BMC and INB and OOB folder path for the script to execute.

- Script excerpt from “SUM_UpgradeGPU_script.sh” for upgrading single GPU system.

```
#Cmd1: Transfer and untar scripts/tools/firmware package

./sum -I Remote_INB -c RemoteExec --oi <OS_IP> --ou <OS_User> --op <OS_Password> --file “HGXA100.tar.gz” --remote_cmd " cd /tmp/ && tar -zxvf HGXA100.tar.gz && cd HGXA100/A100_v0.5"

sleep 5

# Cmd2: check GPU versions

./sum -I Remote_INB -c RemoteExec --oi <OS_IP> --ou <OS_User> --op <OS_Password> --remote_cmd " cd /tmp/HGXA100/A100_v0.5 && chmod +x functions.sh && source ./functions.sh && _generate_firmware_info "

sleep 5

# Cmd3: Inb Update

 ./sum -I Remote_INB -c RemoteExec --oi <OS_IP> --ou <OS_User> --op <OS_Password> --remote_cmd " cd /tmp/HGXA100/A100_v0.5 &&  ./startup_INB.sh"

# Cmd4: OOB Update for CEC or FPGA. (This command will use other SUM command, UpdateGpuFw)

./sum -i <BMC_IP> -u <BMC USER> -p <BMC_PWD> -c UpdateGpu --item <CEC | FPGA> --file <CEC | FPGA file image path>
```

Note: User can also use “SUM_UpgradeGPU_MMscript.sh” under “SUM folder/script/” for upgrading multiple GPU systems.

Appendix L. Creating a Firmware Updating Tar File for OpenBMC

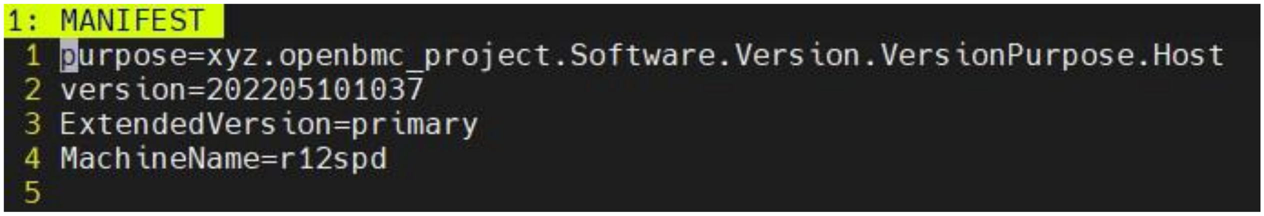
L.1 BIOS Firmware Updating Tar File for OpenBMC

The UEFI firmware update for OpenBMC uses the tar format, which includes the firmware image (*.img format) and a MANIFEST file.

The following steps can be used to create the tar file:

1. Create a MANIFEST file with the following content:

```
purpose=xyz.openbmc_project.Software.Version.VersionPurpose.Host
version=[BIOS_BUILD_DATE]
ExtendedVersion=primary
MachineName=r12spd
```



```
1: MANIFEST
purpose=xyz.openbmc_project.Software.Version.VersionPurpose.Host
version=202205101037
ExtendedVersion=primary
MachineName=r12spd

```

2. Create a tar file including the firmware image and MAINFEST file:

```
$ tar -cvf bios_image.tar bios_image MANIFEST
```

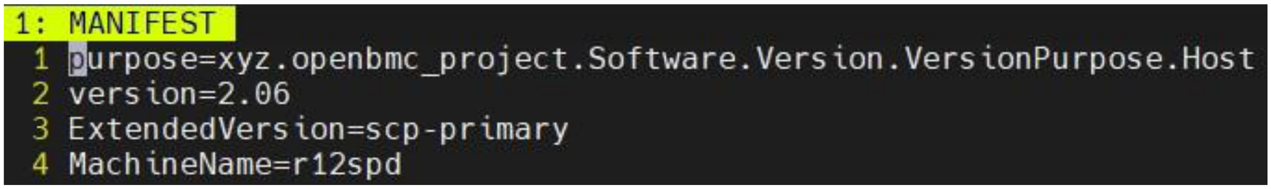
L.2 Ampere SCP Firmware Updating Tar File for OpenBMC

The Ampere SCP firmware for OpenBMC uses the tar format, which includes the firmware image (*.slim format) and a MANIFEST file.

The following steps can be used to create the tar file for installing SCP firmware:

1. Create a MANIFEST file with the following content:

```
purpose=xyz.openbmc_project.Software.Version.VersionPurpose.Host
version=2.06
ExtendedVersion=scp-primary
MachineName=r12spd
```



```
purpose=xyz.openbmc_project.Software.Version.VersionPurpose.Host
version=2.06
ExtendedVersion=scp-primary
MachineName=r12spd
```

2. Create a tar file including the firmware image and MAINFEST file:

```
$ tar -cvf r12spd_atf_xxxx.tar altra_scp_signed_x.xx.xxxxx.slim MANIFEST
```

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