



SuperServer Automation Assistant (SAA)

User's Guide

Revision 1.1.0

Table of contents:

- Version History
- 1. Overview
 - 1.1 Features
 - 1.2 Operations Requirements
 - 1.2.1 OOB Usage Requirements (Remote Management Server)
 - 1.2.2 OOB Usage Requirements (Network)
 - 1.2.3 OOB Usage Requirements (Managed Systems)
 - 1.2.4 In-Band Usage Requirements
 - 1.2.5 Additional In-Band Usage Requirements
 - 1.3 Typographical Conversions
- 2. Installation and Setup
 - 2.1 Installing SAA
 - 2.1.1 Linux, Windows, and FreeBSD
 - 2.1.2 VMware ESXi
 - 2.1.2.1. Installing Redfish Host Interface
 - 2.2 Setting Up OOB Managed Systems
 - 2.2.1 Installing the TAS Package
 - 2.3 Setting Up In-Band Managed Systems
 - 2.3.1 Building a Linux Driver
 - 2.3.2 Signing a Driver in Linux
 - 2.4 Setting Up Remote In-Band Managed Systems
- 3. Licensing Managed Systems
 - 3.1 Getting Node Product Keys from Supermicro
 - 3.2 Activating Managed Systems
 - 3.3 Auto-Activating Managed Systems
- 4. Basic User Interface
 - 4.1. General Options
 - 4.2. Customizing SAA Configurations
 - 4.3. Managing A Single System
 - 4.3.1. OOB
 - 4.3.2. In-Band
 - 4.3.3. Redfish Host Interface
 - 4.3.3.1. AuthNone Authentication

-
- 4.3.3.2. BootStrapping Account feature
 - 4.3.4. Remote In-Band
 - 4.3.4.1. Customizing Remote SAA Configurations
 - 4.3.4.2. Using Remote In-Band (Remote_INB) Mode
 - 4.3.4.3. Using Remote Redfish Host Interface (Remote_RHI)
 - 4.3.4.4. Console Output
 - 4.3.4.5. Supported Commands
 - 4.3.4.6. Transferring Files
 - 4.4. Managing Multiple Systems
 - 4.4.1. Input Output Controls for Multiple Systems
 - 4.4.1.1. File Input
 - 4.4.1.2. File Output
 - 4.4.1.3. Screen Output
 - 4.4.1.4. Log Output
 - 4.5. Command Options
 - 4.5.1. License Management
 - 4.5.2. Health Management
 - 4.5.3. System Management
 - 4.5.4. BIOS Management
 - 4.5.5. BMC Management
 - 4.5.6. System Event Log
 - 4.5.7. CMM Management
 - 4.5.8. Storage Management
 - 4.5.9. Power Management
 - 4.5.10. Applications
 - 4.5.11. GPU Management
 - 4.5.12. CPLD Management
 - 4.5.13. NIC Management
 - 4.5.14. VM Management
 - 4.5.15. NM Management
 - 4.5.16. Multi-Node Management
 - 4.5.17. FPGA Management
 - 4.5.18. PCIeSwitch Management
 - 4.5.19. Security Management
 - 4.5.20. MCU Management

-
- 4.6. SAA Logs
 - 4.7. XML File Format
 - 4.7.1. BIOS Settings XML File Format
 - 4.7.2. BMC Configuration XML File Format
 - 4.7.2.1 Pure Redfish LAN Table in BMC Configuration
 - 4.7.3. BMC LAN Configuration XML File Format
 - 4.7.4. CMM Configuration XML File Format
 - 4.7.5. RAID Configuration XML File Format
 - 4.7.6. Format of the VROC Configuration XML File Format
 - 4.7.7. TwinPro Configuration XML File Format
 - 4.7.8. Fixed Boot Configuration XML File Format
 - 4.8. Text File Format
 - 4.8.1. DMI Information Text File Format
 - 4.9. TUI
 - 4.9.1. TUI General Reminders
 - 4.9.2. BIOS TUI Configuration
 - 4.9.2.1. TUI Display
 - 4.9.2.2. How to Use
 - 4.9.2.3. Getting General Help
 - 4.9.2.4. Loading Previous Values
 - 4.9.2.5. Loading Optimized Values
 - 4.9.2.6. Setting a Password
 - 4.9.2.7. Exiting the TUI
 - 5. Managing Systems
 - 5.1. License Management
 - 5.1.1. Activating the Node Product Keys
 - 5.1.2. Querying the Node Product Keys
 - 5.1.3. Getting and Activating Intel On Demand
 - 5.1.3.1. CpuOnDemand Flow
 - 5.1.3.2. Using the CpuOnDemand Command
 - 5.2. Health Management
 - 5.2.1. Checking OOB Support
 - 5.2.2. Checking Asset Information (OOB Only)
 - 5.2.3. Checking Sensor Data
 - 5.2.4. Checking System Utilization (OOB Only)

-
- 5.2.5. Monitoring the Host with ServiceCalls
 - 5.2.5.1. ServiceCalls XML File Format
 - 5.2.5.2. Email Format
 - 5.2.5.3. Cache File
 - 5.2.6. Monitoring and Controlling PFA of the System
 - 5.2.7. Checking Memory Health of the Managed System
 - 5.2.8. Getting and Clearing the Chassis Intrusion Status for the Managed System
 - 5.2.9. Getting Alert Messages
 - 5.2.9.1. Setting the Destination for Alert Messages
 - 5.2.9.2. Use Alert Sever
 - 5.2.9.3. Getting Alert Message
 - 5.2.9.4. Query Alert Message
 - 5.2.9.5. Send Test Alert
 - 5.2.10. Running Super Diagnostics Offline (SDO) Remotely
 - 5.2.10.1. Running Diagnostics in Embedded Mode
 - 5.2.11. Sending Diag Interrupt
 - 5.2.12. Monitoring CDU Status
 - 5.2.12.1. Getting CDU Information
 - 5.2.12.2. Setting CDU Alert Setting
 - 5.2.12.3. JSON File Format of CDU alert setting
 - 5.2.13. Managing TAS Functionality
 - 5.2.14. Checking and Reporting Basic Health Status of the BMC
 - 5.2.15. Getting and Setting Hardware Debug Tool Status
 - 5.3 System Management
 - 5.3.1 Managing FRU Information
 - 5.3.1.1 Getting FRU Information
 - 5.3.1.2 Restoring FRU Information
 - 5.3.1.3 Changing FRU Information
 - 5.3.2. Getting System Summary Firmware Image Information
 - 5.3.3. Getting System Settings
 - 5.3.4. Updating the System Settings
 - 5.3.5 Getting Fan Mode
 - 5.3.6. Setting the Fan Mode
 - 5.3.7 Controlling the UID of the Managed System

-
- 5.3.8 Obtaining a summary of Firmware Inventory information
 - 5.3.9 Clearing CMOS
 - 5.4. BIOS Management
 - 5.4.1. Getting BIOS Firmware Image Information
 - 5.4.2. Updating the BIOS Firmware Image
 - 5.4.3. Getting Current BIOS Settings
 - 5.4.4. Updating BIOS Settings Based on the Current BIOS Settings
 - 5.4.5. Getting Factory BIOS Settings
 - 5.4.6. Updating BIOS Settings Based on the Factory Settings
 - 5.4.7. Loading Factory BIOS Settings
 - 5.4.8. Getting DMI Information
 - 5.4.9. Editing DMI Information
 - 5.4.10. Updating DMI Information
 - 5.4.11. Setting Up a BIOS Administrator Password
 - 5.4.12. Erasing the BIOS OA Key
 - 5.4.13. Managing Seamless Update Capsule File
 - 5.4.14. Getting SCP Firmware Image Information
 - 5.4.15. Updating the SCP Firmware Image
 - 5.4.16. Getting Fixed Boot Setting
 - 5.4.17. Updating the Fixed Boot Setting
 - 5.4.18. Getting Boot Option
 - 5.4.19. Setting Boot Option
 - 5.4.20. Booting into an ISO Image from an HTTP Server
 - 5.4.21. Getting BIOS POST Codes
 - 5.5. BMC Management
 - 5.5.1. Getting BMC Firmware Image Information
 - 5.5.2. Updating the BMC Firmware Image
 - 5.5.2.1 Updating BMC Firmware with Preservation of BMC Settings
 - 5.5.3. Getting BMC Settings
 - 5.5.3.1 Generating BMC Settings Format Based on Sample File
 - 5.5.4. Updating BMC Settings
 - 5.5.5 Installing BMC Certification
 - 5.5.6. Setting Up a BMC User Password
 - 5.5.7 Getting the BMC KCS Privilege Level
 - 5.5.8 Setting the BMC KCS Privilege Level

-
- 5.5.9. Loading Factory BMC Settings
 - 5.5.10. Setting the BMC Reset Counter
 - 5.5.11. Getting BMC LAN Settings
 - 5.5.12. Updating BMC LAN Settings
 - 5.5.13. Getting the BMC User List
 - 5.5.14. Setting the BMC User List
 - 5.5.15 Bootstrapping an Account for Redfish Host Interface
 - 5.5.16. Managing a RMCP Service Port
 - 5.5.17. Getting and Setting the BMC Host Name
 - 5.5.18. Getting the BMC Session Information
 - 5.5.19 Managing the Redfish Host Interface
 - 5.5.20 BmcWatchDog
 - 5.5.21 Managing Simple Network Management Protocol
 - 5.5.21.1 Getting BMC Simple Network Management Protocol Status
 - 5.5.21.2 Setting Simple Network Management Protocol Server On
 - 5.5.21.3 Setting Simple Network Management Protocol Server Off
 - 5.5.21.4 Getting BMC Simple Network Management Protocol Community String
 - 5.5.21.5 Setting BMC Simple Network Management Protocol Community String
 - 5.6. System Event Log
 - 5.6.1. Getting System Event Log
 - 5.6.2. Clearing the System Event Log
 - 5.6.3. Getting System Maintenance Event Log
 - 5.6.4. Getting Host Crash Dump Log
 - 5.6.5. Clearing System Maintenance Event Log
 - 5.7. CMM Management (OOB Only)
 - 5.7.1. Getting CMM Firmware Image Information
 - 5.7.2. Updating the CMM Firmware Image
 - 5.7.3. Getting CMM Settings
 - 5.7.4. Updating CMM Settings
 - 5.7.5. Setting Up a CMM User Password
 - 5.7.6 Loading the Factory CMM Settings
 - 5.7.7 Getting BBP Firmware Image Information
 - 5.7.8 Updating the BBP Firmware Image

-
- 5.7.9 Getting Current Power Status of Blade System
 - 5.7.10 Setting the Power Status of the Blade System
 - 5.7.11 Managing the Profile Information
 - 5.7.12 Receiving the Switch Firmware Image Information
 - 5.7.13 Updating the Switch Firmware
 - 5.7.14 Rebooting the Switch
 - 5.7.15. Blade Power Supply Unit Management
 - 5.7.15.1. Getting Blade Power Supply Unit Information
 - 5.7.15.2. Getting Blade Power Supply Unit Consumption
 - 5.7.15.3. Getting Blade System Fan Speed
 - 5.7.15.4. Setting Blade System Fan Speed
 - 5.7.15.5. Getting Blade System Fan Mode
 - 5.7.15.6. Setting Blade System Fan Mode
 - 5.7.16 Profile Management
 - 5.7.16.1 Profile Update Rule
 - 5.7.16.2. Profile Management
 - 5.7.16.3. Updating CMM Configurations
 - 5.7.16.4. Updating Blade System Configurations
 - 5.7.17 Getting Blade Summary
 - 5.7.18. Getting the CMM User List
 - 5.7.19. Setting the CMM User List
 - 5.7.20 Updating Dummy Switch Firmware Image
 - 5.8. Storage Management
 - 5.8.1. Getting RAID Firmware Image Information
 - 5.8.2. Updating the RAID Firmware Image
 - 5.8.3. Getting RAID Settings
 - 5.8.4. Updating the RAID Settings
 - 5.8.5. Getting SATA HDD Information (OOB Only)
 - 5.8.6. Getting NVMe Information
 - 5.8.7 Getting PMem Firmware Image Information
 - 5.8.8 Updating the PMem Firmware Image
 - 5.8.9. Getting VROC Settings
 - 5.8.10. Updating the VROC Settings
 - 5.8.11. Controlling an NVMe Device
 - 5.8.12. Getting NVMe Smart Data

-
- 5.8.13. Getting SAS Expander Firmware Image Information
 - 5.8.14. Updating SAS Expander Firmware Image
 - 5.9. Power Management
 - 5.9.1. Getting PSU Information
 - 5.9.2. Updating the Signed PSU Firmware Image Requested by OEM
 - 5.9.3. Getting Current Power Status of a Managed System
 - 5.9.4. Setting the Power Action of a Managed System
 - 5.9.5. Getting ACPI Power Status of a Managed System
 - 5.9.6. Managing Intel Node Manager Policy
 - 5.9.6.1. Managing the Power Policy by Intel Intelligent Power Node Manager
 - 5.9.6.2. Managing the Power Policy by BMC Intel Node Manager
 - 5.9.7. Managing Data Center Manageability Interface
 - 5.9.7.1. Standard Data Center Manageability Interface Specification
 - 5.9.7.2. Intel Intelligent Power Node Manager V2.0
 - 5.9.8. Getting AIOM Standby Power Configuration of the Managed System
 - 5.9.9. Setting AIOM Standby Power Configuration of the Managed System
 - 5.9.10. Getting PSFRU (Power Supply Field Replaceable Unit) Information
 - 5.10. PCIe-Switch Management
 - 5.10.1. Getting PCleSwitch Information
 - 5.10.2. Updating the PCIe Switch Firmware Image
 - 5.11. Applications
 - 5.11.1. Sending an IPMI/IPMB Raw Command
 - 5.11.1.1. IPMI Raw Command
 - 5.11.1.2. IPMB Raw Command
 - 5.11.2. USB Port Accessibility Control
 - 5.11.3. Acquiring USB Port Access Mode (Inband Only)
 - 5.11.4. Dynamically Controlling USB Port Access Mode (Inband Only)
 - 5.11.5. Managing KMS Server Configurations
 - 5.11.6. SOL
 - 5.11.7. Invoking the Redfish API
 - 5.11.8. Remote Execution
 - 5.11.9. Finding BMC Devices (Inband Only)
 - 5.11.10. Managing Found BMC Devices (Inband Only)
 - 5.11.11. Shell Mode

-
- 5.11.12. Prompt
 - 5.11.13. Launching Remote Console
 - 5.11.14. Getting USB Host Controller Information
 - 5.11.15. Updating the USB Host Controller Firmware Image
 - 5.11.16. Remote Screenshot
 - 5.11.17. Remote Keyboard Operation
 - 5.12. GPU Management
 - 5.12.1. Getting GPU Information
 - 5.12.2. Updating the GPU Firmware Image
 - 5.12.3. Diagnosing AMD MI250 GPU System Status
 - 5.12.4. Getting GPU Dump Log Information
 - 5.13. CPLD Management
 - 5.13.1. Getting CPLD Firmware Image Information
 - 5.13.2. Updating the CPLD Firmware Image
 - 5.13.3. Getting Switchboard CPLD Firmware Image Information
 - 5.13.4. Updating Switchboard CPLD Firmware Image
 - 5.13.5. Getting Backplane CPLD Firmware Information
 - 5.13.6. Updating the Backplane CPLD Firmware Image
 - 5.13.7. Getting Fanboard CPLD Firmware Image Information
 - 5.13.8. Updating Fanboard CPLD Firmware Image
 - 5.13.9. Getting AIP CPLD Information
 - 5.13.10. Updating the AIP CPLD Firmware Image
 - 5.13.11. Getting AOM Board CPLD Firmware Image Information
 - 5.13.12. Updating AOM Board CPLD Firmware Image
 - 5.13.13. Getting Miscellaneous CPLD Firmware Image Information
 - 5.13.14. Updating Miscellaneous CPLD Firmware Image
 - 5.13.15. Getting Midplane SBB CPLD Information
 - 5.13.16. Updating the Midplane SBB CPLD Firmware Image
 - 5.13.17. Getting NIC CPLD Firmware Image Information
 - 5.13.18. Updating NIC CPLD Firmware Image
 - 5.13.19. Getting Transitionboard CPLD Information
 - 5.13.20. Updating the Transitionboard CPLD Firmware Image
 - 5.14. NIC Management
 - 5.14.1. Getting Add-On NIC Firmware Image Information
 - 5.14.2. Updating the Add-On NIC Firmware Image

-
- 5.15. Multi-Node Management
 - 5.15.1. Getting TwinPro Settings
 - 5.15.2. Updating TwinPro Settings
 - 5.15.3. Getting Multi-Node EC Firmware Image Information
 - 5.15.4. Updating the Multi-node EC Firmware Image
 - 5.16. VM Management
 - 5.16.1. Providing an ISO Image as a Virtual Media through BMC and File Server
 - 5.16.2. Removing an ISO Image as Virtual Media
 - 5.16.3. Mounting a Floppy Image as Virtual Media from a Local Image File
 - 5.16.4. Unmounting a Floppy Image as Virtual Media from the Managed System
 - 5.16.5. Getting Virtual Media Information from the Managed System
 - 5.16.6. Managing Multiple Virtual Media Devices from the Managed System
 - 5.16.7. Managing Virtual Media Devices in SAA Shell Mode
 - 5.17. NM Management
 - 5.17.1. Managing Intel Management Engine
 - 5.17.1.1. Getting ME Device ID
 - 5.17.1.2. Resetting ME
 - 5.17.1.3. Resetting ME to Default
 - 5.17.1.4. Entering To Update Mode
 - 5.17.1.5. Powering Off ME
 - 5.17.1.6. Self-Test
 - 5.17.1.7. Getting ME Mode
 - 5.17.1.8. Listing ME Images Information
 - 5.17.1.9. Getting Power Information from ME
 - 5.17.1.10. Getting Temperature Information from ME
 - 5.17.2. Managing Node Manager
 - 5.17.2.1. Managing Node Manager by Intel Intelligent Power Node Manager
 - 5.17.2.2. Managing Node Manager by BMC Intel Node Manager
 - 5.17.3 CPU Management
 - 5.17.3.1 Intel Intelligent Power Node Manager V2.0
 - 5.17.3.2 Intel Intelligent Power Node Manager V4.0
 - 5.17.4 Managing Compute Usage Per Second

-
- 5.17.4.1 Getting the CPUS Capability
 - 5.17.4.2 Getting the CUPS Data
 - 5.17.4.3 Getting the CUPS Configuration
 - 5.17.4.4 Getting the CUPS Policies
 - 5.17.4.5 Getting the Core CUPS Utilization
 - 5.17.4.6 Getting the IO CUPS Utilization
 - 5.17.4.7 Getting the Memory CUPS Utilization
 - 5.17.4.8 Setting CUPS Policy
 - 5.17.4.9 Enabling the CUPS Policy
 - 5.17.4.10 Disabling the CUPS Policy
 - 5.17.5. Managing BMC Intel Node Manager
 - 5.17.5.1. Getting a BMC Device ID
 - 5.17.5.2. Getting Power Information from BMC
 - 5.17.5.3. Getting Temperature Information from BMC
 - 5.18. Security Management
 - 5.18.1. TPM Management
 - 5.18.1.1. Getting TPM Information
 - 5.18.1.2. Provisioning the TPM Module
 - 5.18.1.3. Enabling and Clearing the TPM Module Capabilities
 - 5.18.2. Managing BIOS RoT Functions
 - 5.18.3. Managing BMC RoT Functions
 - 5.18.4. Managing CPLD RoT Functions
 - 5.18.5. Managing Remote Attestation
 - 5.18.6. Acquiring the BMC System Lockdown Mode
 - 5.18.7. Setting the BMC System in Lockdown Mode
 - 5.18.8. Managing Secure Boot
 - 5.18.9. Securely Erasing Hard Disks Attached to a RAID Controller
 - 5.18.10. Securely Erasing Hard Disks
 - 5.18.10.1. Execution Modes
 - 5.18.10.2. Securely Erasing an HDD
 - 5.18.10.3. Setting Up an HDD Password
 - 5.18.11. Getting CPU ERoT Firmware Image Information
 - 5.18.12. Updating CPU ERoT Firmware Image
 - 5.18.13. Managing CPU ERoT RoT Functions
 - 5.18.14. Managing Motherboard FPGA RoT Functions

-
- 5.18.15. Getting GPU External RoT (ERoT) Firmware Image Information
 - 5.18.16. Getting SPDM Measurement Information
 - 5.18.17. Managing CMM RoT Functions
 - 5.19. FPGA Management
 - 5.19.1. Getting Motherboard FPGA Firmware Image Information
 - 5.19.2. Updating Motherboard FPGA Firmware Image
 - 5.20. MCU Management
 - 5.20.1. Getting Motherboard MCU Firmware Image Information
 - 5.20.2. Updating Motherboard MCU Firmware Image
 - Appendix A. SAA Exit Codes
 - Appendix B. Management Interface and License Requirements
 - Appendix C. Known Limitations
 - Appendix D. Third-Party Software
 - Appendix E. How to Change BIOS Configurations in XML Files
 - E.1 Numeric
 - E.2 CheckBox
 - E.3 Option
 - E.4 Password
 - E.5 String
 - E.5.1 File Upload
 - E.5.1.1 TLS Certificate
 - E.6 License Requirement
 - Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files
 - F.1 Introduction
 - F.2 Getting/Setting an XML Value (XML Element)
 - F.3 Getting/Setting an XML Value (XML Attribute)
 - Appendix G. Removing Unchanged BIOS Settings in an XML File
 - Appendix H. How to Sign a Driver in Linux
 - Appendix I. BMC/CMM Password Rule
 - I.1 X12/H12 and later platforms except H12 non-RoT systems
 - I.2 CMM
 - Appendix J. System Lockdown Mode Table
 - Appendix K. Using SAA to Run 3rd -Party Tools
 - K.1 LAN NVM update
 - K.2 NVIDIA HGX A100 GPU firmware update package

-
- [Appendix L. Creating a Firmware Updating Tar File for OpenBMC](#)
 - [L.1 BIOS Firmware Updating Tar File for OpenBMC](#)
 - [L.2 Ampere SCP Firmware Updating Tar File for OpenBMC](#)
 - [Appendix M. Component firmware information and update support matrix](#)
 - [Appendix N. GetGpuInfo/UpdateGpu supported platform matrix](#)
 - [Contacting Supermicro](#)

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 1.1.0

Release Date: Aug 14, 2024

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

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

Copyright © 2024 by Super Micro Computer, Inc.

All rights reserved.

Printed in the United States of America

Version History

Date	Rev	Description
May-16-2024	1.0.0	1. Created this document.
Aug-14-2024	1.1.0	<ol style="list-style-type: none">1. Added the --type option to support RAID type for Broadcom devices for the UpdateRaidController command.2. Added the GetGpuInfo and UpdateGpu commands for Intel Gaudi 3 system.3. Added the RemoteKeyboard command.4. Added the GetMidplaneSbbCpldInfo and UpdateMidplaneSbbCpld commands.5. Added the VMShell command.6. Added the --fru_version option and --item ALL usage to the ChangeFruInfo command.7. Added the --format option to the GetFruInfo and RestoreFruInfo commands.8. Supported MI300X item in the GetGpuLog command.9. Added the UpdateDummySwitch command.10. Added the GetNICCpldInfo and UpdateNICCpld commands.11. Supported Broadcom RAID 3408 and 4116 for the UpdateRaidController command.12. Add the options --usb and --action List for the SuperDiag command.13. Supported MGX_GPU, MI300X, and ONBOARD_RETIMER items in the UpdateGPU command.

1. Overview

The SuperServer Automation Assistant (SAA) is designed to manage Supermicro systems. It helps IT administrators to easily manage the firmware image update and configuration update on the firmware of a system, including BIOS/BMC/CMM/PSU/BBP/RAID/Aoc NIC/GPU/switch/AIP/SCP. In addition, system checks as well as event log management are also supported. Moreover, advanced applications are also provided to facilitate system management. To update configurations, users can edit system BIOS configurations, DMI information and BMC/RAID/CMM configurations from readable text files, as well as use this update manager to apply these configurations.

The SAA supports either Redfish or IPMI, or both industry standards for system management, it varies depending on the BMC of each generation platform. Users are able to manage BMC-based systems in the remote console through out-of-band (OOB) channel or in the local host through in-band channel. It also provides one-to-many configuration management for mass deployment and management.

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.
- License Management
 - Activates the node product key of the managed system.
 - Queries the node product key of the managed system.
 - Gets and activates Intel® CPU On Demand Capabilities features.
- Health Management
 - Gets the OOB feature capabilities of the managed system.

-
- Gets the asset information of the managed system.
 - Gets the utilization rates of the managed system components.
 - Gets the IPMI sensor values of the managed system.
 - Monitors the status of system event log and sensor data record of the managed system.
 - Monitors and controls the predictive failure analysis of the managed system.
 - Sets the memory health checking function of the managed system.
 - Gets and clears the chassis intrusion status for the managed system.
 - Gets and query SNMP trap message.
 - Runs Super Diagnostics Offline (SDO) and checks results.
 - Sends Diag Interrupt.
 - Monitors CDU system to get status and set settings remotely.
 - Executes TAS-related actions.
 - Checks and reports the basic health status of the BMC.
 - Gets and sets the hardware debug tool status.
 - System Management
 - Gets the FRU information of the managed system/input dumped FRU file.
 - Restores dumped FRU info to the managed system.
 - Updates FRU information.
 - Obtains a summary of information from the managed system.
 - Gets the system configuration (BIOS and BMC) of the managed system.
 - Updates the system configuration (BIOS and BMC) of the managed system.
 - Gets the fan configuration of the managed system.
 - Sets the fan configuration of the managed system.
 - Executes command to control UID.
 - Obtains a summary of Firmware Inventory information from the managed system.
 - Executes the command to clear the CMOS.
 - BIOS Management
 - Updates BIOS.
 - Gets the BIOS information of the managed system/input BIOS image file.

-
- Gets the default factory BIOS configuration of the managed system.
 - Gets the current BIOS configuration of the managed system.
 - Updates the BIOS configuration.
 - Loads the default factory BIOS configuration.
 - Gets the DMI information of the managed system.
 - Edits the given DMI information text file.
 - Updates DMI information.
 - Sets BIOS Administrator password.
 - Erases OA key of the managed system.
 - Gets the SCP information of the managed system.
 - Updates SCP.
 - Gets the BIOS fixed boot order configuration of the managed system.
 - Gets BMC boot Information.
 - Sets BMC boot Status.
 - Boots into an ISO image from the image file server.
 - Updates the BIOS fixed boot order.
 - Gets BIOS POST code.
 - BMC Management
 - Updates BMC.
 - Gets the BMC information of the managed system/input BMC image file.
 - Gets the BMC configuration of the managed system.
 - Updates BMC configuration.
 - Gets the BMC LAN configuration of the managed system.
 - Updates BMC LAN configuration.
 - Sets BMC user password.
 - Gets the BMC KCS privilege of the managed system.
 - Sets KCS Privilege.
 - Loads the default factory BMC configuration.
 - Sets BMC reset delay by minute.
 - Gets/Sets BMC user list.

-
- Executes BMC user related actions.
 - Gets/Deletes the Redfish Host Interface login bootstrapping account.
 - Sets RMCP status of managed system.
 - Gets the BMC IPMI session information of the managed system.
 - Gets/Sets the BMC host name.
 - Get/Set the USB Connection for Redfish Host Interface communication.
 - Sets WatchDog timer.
 - Executes command to manage SNMP.
 - System Event Log
 - Gets the event log of the managed system.
 - Clears the event log of the managed system.
 - Gets the Maintenance Event Log of the managed system.
 - Clears the maintenance event log of the managed system.
 - Gets the crash dump of the managed system. Note: the crash dump file is compressed.
 - CMM Management
 - Updates the CMM with the given image file.
 - Gets the CMM information of the managed system/input CMM image file.
 - Gets the CMM configuration of the managed system.
 - Updates the CMM configuration.
 - Sets CMM user password.
 - Loads the default factory CMM configuration.
 - Gets the BBP information of the managed system/input BBP image file.
 - Updates the BBP with the given image file.
 - Gets current power status of blade system.
 - Controls the power status of CMM system.
 - Manages the profiles of the CMM and Blade configuration on CMM.
 - Gets the switch information of the managed system/input switch image file.
 - Updates switch firmware.
 - Reboots the Switch.
 - Manages the power supply unit of managed Blade system through CMM.

-
- Gets/Sets CMM user list.
 - Storage Management
 - Gets the RAID controller information of the managed system/input RAID image file.
 - Updates the RAID controller.
 - Gets the RAID configuration of the managed system.
 - Updates the RAID configuration.
 - Gets the SATA HDD information from the on-board AHCI controller on the managed system.
 - Gets the NVMe SSD information of the managed system.
 - Gets the PMem information of the managed system/input PMem image file.
 - Updates PMem firmware.
 - Gets the VROC configuration of the managed system.
 - Updates the VROC configuration.
 - Locates, inserts or removes NVMe SSD drive.
 - Gets the NVMe smart data of the managed system.
 - Gets the SAS Expander information of the managed system.
 - Updates the SAS Expander.
 - Power Management
 - Prints the PSU information on the managed system.
 - Updates PSU module with the OEM requested signed firmware image.
 - Gets current power status of managed system.
 - Sets power action of managed system.
 - Manages the system by Data Center Manageability Interface (DCMI).
 - Manages the power policy of the managed system.
 - Gets ACPI (Advanced Configuration and Power Interface) status of managed system.
 - Gets AIOM Standby Power configuration of the managed system.
 - Sets AIOM Standby Power configuration of the managed system.
 - PCIe-Switch Management

-
- Gets the PCIe Switch information of the managed system/input PCIe Switch image file.
 - Updates PCIe switch firmware.
 - Applications
 - Sends IPMI raw command.
 - Shows current USB access mode.
 - Sets current USB access mode.
 - Manages KMS server network configurations.
 - Calls Redfish API directly.
 - Executes shell commands on a remote system.
 - Executes SOL related commands.
 - Uses this command to find and display all BMC devices.
 - GPU Management
 - Gets the GPU information of the managed system.
 - Updates Delta/Delta-Next/PVC/Gaudi 2/Gaudi 3/CG1 MGX/MI300X GPU firmware.
 - Diagnoses the AMD MI250 GPU status of the managed system.
 - Gets the GPU log of the managed system.
 - CPLD Management
 - Gets the CPLD information of the managed system/input CPLD image file.
 - Updates CPLD.
 - Gets the Switchboard CPLD information of the managed system.
 - Executes update Switchboard CPLD based on type selected.
 - Gets the backplane CPLD information of the managed system.
 - Updates Backplane CPLD.
 - Gets the Fanboard CPLD information of the managed system.
 - Executes update Fanboard CPLD based on type selected.
 - Gets the AIP (AI Processor) CPLD information of the managed system.
 - Updates CPLD of AIP (AI Processor).
 - Gets the AOM CPLD information of the managed system.
 - Updates CPLD of AOM.

-
- Gets the Miscellaneous CPLD information of the managed system.
 - Updates Miscellaneous CPLD.
 - Gets the Midplane SBB CPLD information of the managed system.
 - Updates the Midplane SBB CPLD.
 - Gets the NIC CPLD information of the managed system.
 - Updates the NIC CPLD.
 - Gets the Transitionboard CPLD information of the managed system.
 - Updates the Transitionboard CPLD.
 - NIC Management
 - Gets the AOC NIC information of the managed system/input AOC_NIC image file.
 - Updates AOC NIC FW.
 - Multi-Node Management
 - Gets the TwinPro information of the managed system.
 - Updates the TwinPro configuration.
 - Gets the multi-node EC information of the managed system/input multi-node EC image file.
 - Updates multi-node EC.
 - VM Management
 - Mounts an ISO image from the image file server.
 - Unmounts the ISO image resources.
 - Mounts a floppy image from the given file.
 - Unmounts the floppy image file of the managed system.
 - Gets the virtual media information of the managed system.
 - Manages the virtual media devices of the managed system.
 - NM Management
 - Manages Intel Management Engine of managed system.
 - Manages Intel Node Manager of managed system.
 - Manages the CPU of managed system.
 - Manages the Compute Usage Per Second(CUPS) of managed system.
 - Security Management

-
- Executes RoT-related actions.
 - Sets secure boot.
 - Gets system lockdown status.
 - Sets system lockdown mode.
 - Attests managed system and manages measurements.
 - Securely erases RAID HDDs in RAID storage system.
 - Securely erases hard disks for the managed system.
 - Launches the trusted platform module provision procedure.
 - Gets TPM information of the managed system.
 - Manages the trusted platform module of the managed system.
 - Gets the CPU ERoT information of the managed system.
 - Updates CPU ERoT.
 - Gets the SPDm information of the managed system.
 - FPGA Management
 - Gets the motherboard FPGA information of the managed system.
 - Updates FPGA of motherboard.
 - MCU Management
 - Gets the motherboard MCU information of the managed system.
 - Updates MCU of motherboard.

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 5.11 (x86_64) or later Linux: CentOS 5.11 (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 9.0 (aarch64) or later Linux: Oracle Linux 9.0 (aarch64) or later Linux: Rocky Linux 9.0 (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 12 (x86_64) or later ESXi: ESXi 7.0 and ESXi 8.0

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)

SAA 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	X12 ATEN platform (SMT_X12): 1.00 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	Version 1.0 or later for select X12 3rd Generation Intel® Xeon® Scalable processors with Intel® C620 Series Chipsets Product Family X12/H12 or later 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_1x.3x_20170802yyyymmdd.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 and TasManage commands require additional packages to be installed on the managed system.

Program/Script	Description	Privilege Requirement
TAS_x.x.x_build.yymmdd.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.

Pre-requisite for TAS to be installed successfully on the managed system. System Requirements please refer to [TAS user guide](#).

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

Firmware Image	Requirements
BMC Version	X12 ATEN platform (SMT_X12): 1.00 or later H12 ATEN platform (SMT_H12): 1.00 or later

1.2.4 In-Band Usage Requirements

With the use of in-band, SAA 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	<p>BIOS Version 1.0 or later for X12/H12 select systems</p> <p>BIOS Version 1.0d or later for Ampere® Altra®/Altra® Max processor family on R12 platforms</p>
Operating System	<p>Linux: Red Hat Enterprise Linux 5.11 (x86_64) or later</p> <p>Linux: CentOS 5.11 (x86_64) or later</p> <p>Linux: Ubuntu 12.04 LTS (x86_64) or later</p> <p>Linux: Debian 7 (x86_64) or later</p> <p>Linux: SUSE Linux Enterprise Server 12 SP3 or later</p> <p>Linux: Red Hat Enterprise Linux 9.0 (aarch64) or later</p> <p>Linux: Oracle Linux 9.0 (aarch64) or later</p> <p>Linux: Rocky Linux 9.0 (aarch64) or later</p> <p>Linux: Debian 11.1.0 (aarch64) or later</p> <p>Linux: Ubuntu Server 20.04.3 (aarch64) or later</p> <p>Windows: From Windows Server 2008 R2 SP1 (x64) to Windows Server 2019</p> <p>FreeBSD: FreeBSD 12 (x86_64) or later</p> <p>ESXi: ESXi 7.0 and ESXi 8.0</p>

**Note:**

Though SAA 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
SAA Execution Privilege	To execute in-band functions, SAA 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	SAA	The main program for SAA
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	X12 ATEN platform (SMT_X12): 1.00 or later H12 ATEN platform (SMT_H12): 1.00 or later R12 OpenBMC platform: 2.9.1-v27 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 12 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 Conventions

This manual uses the following typographical conventions.

Convention	Definition
Bold	Keywords needing attention are in bold.
<i>Italics</i>	Variables and section names are in italics.

{ }	Curly braces indicate that at least one of the enclosed items is required.
[]	Square brackets indicate that the enclosed item or items are optional.
< >	Angle brackets enclose the parameters in the syntax description.
	A vertical bar separate the items in a list.
Courier-New font size 10	represents Command Line Interface (CLI) instructions in Linux terminal mode.
[shell]#	represents the input prompt in Linux terminal mode.
[SAA_HOME]#	represents the SAA home directory prompt in Linux terminal mode.

- **Obligatory choices**

Curly braces and vertical bars – choose only one option.

{ --enable | --disable }

- **Optional choices**

One item in square brackets – You can choose it or omit it.

[--overwrite]

Square brackets and vertical bars – choose none or only one.

[--load_unique_password | --load_default_password]

2. Installation and Setup

2.1 Installing SAA

2.1.1 Linux, Windows, and FreeBSD

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

1. Extract the `saa_x.x.x_Linux_x86_64_YYYYMMDD.tar.gz` archive file.
2. Go to the extracted `saa_x.x.x_Linux_x86_64` directory. Name this directory as "SAA_HOME".
3. Run SAA in the SAA_HOME directory.

Linux Example:

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

```
[shell]# cd saa_x.x.x_Linux_x86_64
```

```
[SAA_HOME]# ./saa
```



Note:

It is recommended that SAA tool with SAA release package should be used because binary files are required for certain commands.

2.1.2 VMware ESXi

To install SAA user world tool and driver in ESXi, follow these steps.

1. Copy the component bundle to the ESXi server. Technically, you can place the file anywhere that is accessible to the ESXi console shell, but for these instructions, we'll assume the location is in '/tmp'.

-
- Here's an example of using the Linux 'scp' utility to copy the file from a local system to an ESXi server located at 10.10.10.10:
- ```
scp SMC-ESXi-uw-saa_1.0.0-0.1.001_22026697.zip root@10.10.10.10:/tmp
```
2. Issue the following command (full path to the file must be specified):  
`esxcli software component apply {Component_File}`  
In the example above, this would be:  
`esxcli software component apply -d /tmp/SMC-ESXi-uw-saa_1.0.0-0.1.001_22026697.zip`
  3. scp ESXi driver to datastore  
Here's an example of using the Linux 'scp' utility to copy the file from a local system to an ESXi server located at 10.10.10.10:  

```
scp Supermicro-vmware-phymem-driver_1.0-0.0.0001_22037294-package.zip root@10.10.10.10:/vmfs/volumes/datastore1
```
  4. Set .saarc ESXi\_driver variable like below:  
`ESXi_driver = /vmfs/volumes/datastore1/Supermicro-vmware-phymem-driver_1.0-0.0.0001_22037294-package.zip`
  5. ESXi firewall is enabled by default, please setup the whitelist in ESXi system. You can refer to  
2.1.2.1 Installing Redfish Host Interface, if the managed system does not support redfish host interface, you do not need to add this line "sh /opt/supermicro/bin/network.sh" in /etc/rc.local.d/local.sh file.

#### 2.1.2.1. Installing Redfish Host Interface

The network.sh and custom\_service.xml are included in the component package. Follow these steps to set up the network configuration and reboot the system after completing the settings.

1. Add the "cp /vmfs/volumes/datastore1/custom\_service.xml /etc/vmware/firewall/esxcli network firewall refresh sh /opt/supermicro/bin/network.sh" commands to the /etc/rc.local.d/local.sh file in ESXi system.

---

```
#!/bin/sh ++group=host/vim/vmvisor/boot

cp /vmfs/volumes/datastore1/custom_service.xml /etc/vmware/firewall/
esxcli network firewall refresh
sh /opt/supermicro/bin/network.sh
```

2. Check if the firewall settings are suitable for your ESXi system.
3. Copy /etc/vmware/firewall/service.xml to your /vmfs/volumes/datastoreX, where X represents a variable (the specific number may vary on your ESXi system.)
4. Rename the “service.xml” file to “custom\_service.xml” and use this file to create a whitelist.
5. In the SAA package, find the firewall whitelist setting in /opt/supermicro/bin/custom\_service.xml, compare these settings with the default settings in /etc/vmware/firewall/service.xml in your system.
6. The webAccess service should be enabled by default. Check the status of the webAccess on your system.
7. Open the /opt/supermicro/bin/custom\_service.xml file, locate the “webAccess service” keyword, and add this rule between <rule id=0000>and <rule id=0007>:

```
<rule id='0000'>
 <direction>inbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>80</port>
</rule>
<rule id='0001'>
 <direction>inbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>443</port>
</rule>
<rule id='0002'>
 <direction>inbound</direction>
 <protocol>udp</protocol>
 <porttype>dst</porttype>
 <port>623</port>
</rule>
```

---

```
<rule id='0003'>
 <direction>outbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>80</port>
</rule>
<rule id='0004'>
 <direction>outbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>443</port>
</rule>
<rule id='0005'>
 <direction>outbound</direction>
 <protocol>udp</protocol>
 <porttype>dst</porttype>
 <port>623</port>
</rule>
<rule id='0006'>
 <direction>outbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>25</port>
</rule>
<rule id='0007'>
 <direction>inbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>25</port>
</rule>
```



```

<service id='0015'>
 <id>webAccess</id>
 <rule id='0000'>
 <direction>inbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>80</port>
 </rule>
 <rule id='0001'>
 <direction>inbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>443</port>
 </rule>
 <rule id='0002'>
 <direction>inbound</direction>
 <protocol>udp</protocol>
 <porttype>dst</porttype>
 <port>623</port>
 </rule>
 <rule id='0003'>
 <direction>outbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>80</port>
 </rule>
 <rule id='0004'>
 <direction>outbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>443</port>
 </rule>
 <rule id='0005'>
 <direction>outbound</direction>
 <protocol>udp</protocol>
 <porttype>dst</porttype>
 <port>623</port>
 </rule>
 <rule id='0006'>
 <direction>outbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>25</port>
 </rule>
 <rule id='0007'>
 <direction>inbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>25</port>
 </rule>
 <enabled>true</enabled>
 <required>false</required>
</service>

```

8. After applying the above settings, reboot the system.



#### Notes:

- The /vmfs/volumes/datastoreX folder might be different in ESXi system. Please check it in your ESXi system first.
- The custom\_service.xml must be located in the datastore folder, and the XML file path must be same as the setting in

---

/etc/rc.local.d/local.sh file.

- X13 and later platforms may have Redfish Host Interface problem, users can set RC “hostinterface\_enable” variable in the .saarc file. Please see 4.2. Customizing SAA Configurations.
- 

## 2.2 Setting Up OOB Managed Systems

To set up 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 SAA 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 SAA “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” and “TasManage” commands only).

### 2.2.1 Installing the TAS Package

The TAS package (TAS\_version\_build.date.zip) can be acquired from [Supermicro](#). Windows, Linux, FreeBSD, and ESXi platforms are supported. To install TAS, please refer to [TAS user guide](#).

## 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, SAA 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 SAA\_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 supermicro_phymem.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 supermicro_phymem.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.
  - < **private key name** >.der: the generated public key file name.
-

---

## 2.4 Setting Up Remote In-Band Managed Systems

Remote In-Band management involves sending commands via SSH and transferring files via SFTP to the remote managed systems.



To set up Remote In-Band managed systems, follow these steps:

1. **Install and Start OpenSSH Server:** Ensure the OpenSSH server service is installed and running on the managed systems. This is critical for enabling secure command execution and file transfers.
2. **Configure Firewall Settings:** Configure the firewall settings on the managed systems to allow SSH access. This ensures that the systems can receive and respond to SSH commands and SFTP file transfers.
3. **Verify Installation and Configuration:** Check that the OpenSSH server is operational by testing an SSH connection to the managed system. Use the following command format:

```
[shell]# ssh <username>@<IP or hostname>
```

For more detailed information on OpenSSH, please visit the [OpenSSH official website](#).



**Note:** Make sure Remote In-Band managed systems meet the requirements in 1.2.4 In-Band Usage Requirements.

---

---

## 3. Licensing Managed Systems

---

Each node is licensed by a product key. To access most SAA 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 SAA. 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 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. SAA also provides 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":"1111111111111111111122222222222223
333333333333abababababababababababbabcdcdcdcdcdccdcddcdefefefefefe
fefefefefefghghghghghghghghghghghgh"}}}
```

## 3.2 Activating Managed Systems

To activate a single system or simultaneously activate multiple systems, see 5.1.1 Activating the Node Product Keys.

### 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 Supermicro 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 Supermicro sales representative to obtain a credential file ("cred.bin").
  3. Put the credential file in the "SAA\_HOME/credential" directory on the system where the required SAA command is run.
  4. SAA 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

---

SAA 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:

```
[SAA_HOME]# ./saa
```

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

```
[SAA_HOME]# ./saa -h -c <command name>
```

Example:

```
[SAA_HOME]# ./saa -h -c UpdateBios
```

### 4.1. General Options

SAA offers a range of general options, allowing you to manage the program's behavior according to their specific requirements. These options include BMC/CMM login authentication, configurations for remote SSH execution, and output verbosity.

Options	Description or usage
-h	Shows help information.
-v	Displays the verbose output on the screen.
-l	<InterfaceName> (case sensitive) Supported Interfaces: 1. Redfish_HI = Executes In-Band commands through Redfish Host Interface. 2. Remote_INB = Executes In-Band commands on remote systems. 3. Remote_RHI = Executes In-Band commands through 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>
--oi	<OS IP address>
--ou	<OS user ID>
--op	<OS user password>
--os_key	<OS private key>
--os_key_pw	<OS private key password>
--batch_count	<Number of executions in a single batch> (For managing multiple systems only)
--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 .saarc 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 SAA journal level> (0: silent, 1: fatal, 2: error, 3: warning, 4: information, 5: debug, 6: verbose)
--journal_path	<set SAA journal path>

--rc_path	<set .saarc file path>
--show_multi_full	Shows the intermediate status of all managed systems. (For multiple systems, only OOB managed systems are shown.)
--remote_saa	<sets remote SAA path> (For remote in-band usage)
--remote_saa_rc	<sets .saarc file path in the remote system> (For remote in-band usage)



**Note:**

For the reboot option, SAA applies the managed system to reboot or power up after executing the command properly. If the SAA command throws exception, the system may not reboot or power up. After the command is executed, users must check the reboot function is correctly executed.

## 4.2. Customizing SAA Configurations

Two methods allow you to customize execution configurations, command options and the .saarc file. A command option precedes a .saarc file. In other words, a parameter in the .saarc file will be overwritten by a corresponding parameter in a command option. The default configuration applies when there is no assignment or validity in the command option or .saarc. The table below provides a summary of the customizable 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 the .saarc file

journal_path	[1]Linux: ~/journal/supermicro/saa/, [1]Windows: %HomePath%\journal\supermicro\saa\	Sets the journal output path. When the journal level is set to 0 (silent), this parameter will be invalid.	Both command option and the .saarc file
confirm_timeout	[1]300	[2]Sets the confirm flag polling timeout. The unit is second.	the .saarc file only
udp_timeout	[1]240	Sets the timeout for checking UDP connections in seconds. The value should be between 1 and 240, inclusive.	the .saarc file only
thread_count	[1]50	[3]Sets the thread count.	the .saarc file only
multi_retry_count	[1]2	Sets retry count for using executions on multiple systems.	the .saarc file only
ipv6_file_name_switch	[1]0: disable, 1: enable	Replaces ':' (colon) with ' ' (two single quotation marks) when the file name contains an IPv6 address.	the .saarc file only
cache_path	[1]%WorkingDirectory%	[4]Sets the cache file path of ServiceCalls.	the .saarc file only
https_port	[1]443	[5]Sets the managed system's HTTPS port.	the .saarc file only
certificate	None	[6]Sets the certificate files to verify the customized and signed RoT firmware images.	the .saarc file only

rmcp_port	[1]623	Sets managed system RMCP port for CMM/BMC connection.	Both command option and .saarc file
post_timeout	[1]1200	Sets post complete polling timeout.	.saarc file only
config_default_action	[1]none	Sets the default action of XML config file that GetBmcCfg and GetCmmCfg generated. Acceptable value (case insensitive): none, change.	Both command option and .saarc file
hostinterface_enable	[1]on	Sets the host interface enable by SAA.	.saarc file only
Network_controller	[1]RNDIS	Sets Redfish Host Interface USB connection to CDC_ECM or RNDIS.	.saarc file only
db_path	[1]Linux: ./GO_SNMP/default.db [1]Windows: .\GO_SNMP\default.db	Configures AlertManage to read the location of the SQLite database file.	the .saarc file only
ESXi_driver	[1]/vmfs/volumes/datastore1/Supernova-vmware-summary_1.0-0.0.0001_21624800.zip	Sets ESXi driver absolute path.	the .saarc file only
max_upload_speed	[1]1000	Sets the maximum upload speed for uploading firmware files in multiple-node mode. Speed is measured in Mbp/s.	the .saarc file only

---

		The default value is 1000 Mbps.	
vm_port	[1]623	Sets managed system Virtual Media port.	the .saarc file only
ikvm_port	[1]5900	Sets managed system IKVM Server port.	the .saarc file only

[1]The default configuration value.

[2]When a file is uploaded to BIOS via BMC, SAA will continuously check for successful BIOS updates after rebooting. If, within the confirmed\_timeout seconds, SAA does not receive a "success" message, it stops polling and displays a message indicating that the file is "being updated." This suggests that the system requires additional time to boot up. To ensure SAA receives a "success" message before timing out, consider increasing the confirmed\_timeout.

[3]SAA can limit its maximum concurrent executing count to prevent a system from overloading. The thread\_count in the .saarc file can be adjusted to protect the system during the execution of SAA in multiple-node mode. For example, setting the thread count to 50 means that SAA will execute 50 working threads simultaneously.

[4]Accessing cache files on mounted file systems using the ServiceCalls command is not supported. Ensure that the target path is not within 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.

[7]When the setting value is 0, the upload speed is not limited.

There are three ways to specify the .saarc file: through the command option --rc\_path (highest priority), the .saarc file in the current directory (intermediate priority) and the .saarc in the user home directory (lowest priority). You can rename the saarc.sample file to ".saarc" in the current directory or move the file to the user home directory and rename to .saarc based on user's requirements. Note that a .saarc sample

---

configuration file is bundled with the SAA release package. An example is provided below.

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

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

set SAA 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

set managed system RMCP port for CMM/BMC connection
#rmcp_port = 623

set post complete polling timeout
#post_timeout = 1200

set the default action of XML config file that GetBmcCfg and GetCmmCfg
generated
Acceptable value (case insensitive): none, change
#config_default_action = none

set the host interface enable by SAA
#hostinterface_enable = on
```

---

```
set Redfish Host Interface USB connection to CDC_ECM or RNDIS
#Network_controller = RNDIS

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

set the default action of XML config file that GetBmcCfg and GetCmmCfg
generated
Acceptable value (case insensitive): none, change
#config_default_action = none

set the host interface enable by SAA
#hostinterface_enable = on

set Redfish Host Interface USB connection to CDC_ECM or RNDIS
#Network_controller = RNDIS

set snmp sqlite file path
#db_path = ./GO_SNMP/default.db

set ESXi driver absolute path
#ESXi_driver = /vmfs/volumes/datastore1/Supermicro-vmware-sum-driver_1.0-
0.0.0001_21624800.zip

set the maximum upload speed for uploading firmware file in multiple node mode.
Speed is measured in Mbit/s. Default value is 1000 Mbps
#max_upload_speed = 1000

set managed system Virtual Media port
#vm_port = 623

set managed system IKVM Server port
#ikvm_port = 5900
```

The syntax "name=value" represents the parameter name defined by SAA, and "value" is the parameter value that can be configured. If a parameter value is considered invalid, SAA will ignore it. By default, all parameters in .saarc are deactivated, and the "#" (pound mark) at the beginning of a line may be removed to activate a parameter configuration.



**Note:**

In Windows, copy the SAA configuration file and rename it to .saarc using Command Prompt.

---

---

## 4.3. Managing A Single System

In this section, we describe the basic user operations for managing a single system, either through the OOB channel or, if applicable, through the In-Band or In-Band Redfish Host Interface channel. For detailed on the usage of each command, please see 5. Managing Systems.

### 4.3.1. OOB

For managing a system through the OOB channel, the -i, -u, -p options are used for BMC login authentication.

Syntax:

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c <command> [command options]

Example:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBmcInfo
```

Alternatively, you can use the -f option to specify a user password file, eliminating the need to manually enter the password each time. For simplicity, only the first syntax will be presented in the subsequent content.

Single System	
OOB	saa -i <IP or host name> -u <username> -f <password file> -c <command> [command options]

Example:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -f Password.txt -c GetBmcInfo
```

Password.txt





---

111111

### 4.3.2. In-Band

For managing a system through the In-Band channel, simply use the -c option to execute a command and do not use the -l, -i, -u, -p and -f options. To check the In-Band supported commands and their node product key requirement, please see Appendix B. Management Interface and License Requirements.

Syntax:

Single System	
In-Band	saa -c <command> [command options]

Example:

```
[SAA_HOME]# ./saa -c GetBmcInfo
```

### 4.3.3. Redfish Host Interface

The 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 the Redfish Host Interface, refer to the Redfish Host Interface Specification by DMTF.

Some commands support the Redfish Host Interface.



#### Notes:

- The Redfish Host Interface is not enabled by default in Linux. To enable the Redfish Host Interface in Linux/FreeBSD, Linux\_enable\_RHI.sh and FreeBSD\_setup\_RHI.sh in the SAA release package under the /script folder.
- For SUSE12 systems, if the Redfish Host Interface is still not working after Linux\_enable\_RHI.sh is enabled, you can execute SuSE12\_Firewall\_WhiteList.sh in the SAA release package under /script/SUSE to add the Redfish Host Interface to the firewall whitelist.

- For ESXi systems, please see 2.1.2.1 Installing Redfish Host Interface.

Syntax:

Single System	
In-Band	saa -I Redfish_HI -u <username> -p <password> -c <command> [command options]

Example:

```
[SAA_HOME]# ./saa -I Redfish_HI -u <username> -p <password> -c GetBmcInfo
```

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

#### 4.3.3.1. AuthNone Authentication

SAA supports 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 SAA commands supporting -I Redfish\_HI without BMC username and password.

Syntax:

Single System	
In-Band	saa -I Redfish_HI -c <command> [command options]

Example:

```
[SAA_HOME]# ./saa -I Redfish_HI -c GetBmcInfo
```

#### 4.3.3.2. BootStrapping Account feature

SAA supports bootstrapping account feature for in-band Redfish Host Interface which allows users to execute all SAA commands supporting -I Redfish\_HI without entering BMC username and password. A bootstrapping account will be created and recorded in

---

a cache file, if AuthNone authentication is not supported by the managed system. SAA will use the account listed in the cache file to log in and execute the SAA command.

Syntax:

Single System	
In-Band	saa -I Redfish_HI -c <command> [command options]

Example:

```
[SAA_HOME]# ./saa -I Redfish_HI -c GetBmcInfo
```

**The console output contains the following information:**

```
Writing username and password to BootstrappingAcc file.
```

```
Managed system.....169.254.3.254
 BMC type.....X12_RoT_ATEN_AST2500
 BMC version.....00.23.37
 BMC ext. version.....01 00 00 (P)
 BMC build date.....2021/06/28
```

### 4.3.4. Remote In-Band

You can remotely run in-band commands on remote systems in Remote In-Band mode.



**Notes:**

- To run commands in this mode, make sure the remote managed system meet the requirements in 2.4 Setting Up Remote In-Band Managed Systems.
- In addition, if the remote managed system is FreeBSD, the sudo command must be installed by using "pkg install sudo".

---

#### 4.3.4.1. Customizing Remote SAA Configurations

To execute Remote In-Band commands on a remote system, the path to the remote SAA executable must be specified. The remote SAA path can be specified in three

---

ways. The priority applies from high to low.

1. Firstly, use the `--remote_saa` command option to specify the path to the remote SAA executable when executing Remote In-Band commands. For example,

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op
111111 -c GetBmcInfo --remote_saa /root/saa
```

2. Secondly, rename the `remoteSaarc.sample` file to `".remoteSaarc"` and copy it to `${HOME}/supermicro/.remoteSaarc` in the remote system, and specify the `remote_saa_path` setting.
3. Finally, if none of the above methods are employed, you can place the remote SAA in the default path in `${HOME}/supermicro/saa` in the remote system.

More configurable settings for remote SAA are summarized below:

Setting Name	Setting Value Sample	Description	Customized Methods
remote_saa_path	Linux and FreeBSD: ~/supermicro/saa  Windows: %HomePath%\supermicro\saa.exe  VMware ESXi: /opt/supermicro/bin/saa	Sets the remote SAA path	--remote_saa command option and .remoteSaarc file
remote_folder	Linux and FreeBSD: ~/supermicro  Windows: %HomePath%\supermicro  VMware ESXi: /vmfs/volumes/dat	Sets the file transfer folder for remote SAA execution	.remoteSaarc file only

	astore1/supermicro		
--	--------------------	--	--

In addition, to execute remote in-band commands with customized execution configurations, refer to *4.2 Customizing SAA Configurations*. Instead of the `--rc_file` option, use the `--remote_saa_rc` option to specify the `.saarc` file path on the remote system.

#### 4.3.4.2. Using Remote In-Band (Remote\_INB) Mode

Syntax:

Single System	
Remote In-Band	<code>./saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS user ID&gt; --op &lt;OS user password&gt; -c &lt;command&gt; [command options]</code>

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

Alternatively, you can use the `--os_key` and `--os_key_pw` options to log in to a remote system through a private key. For simplicity, only the first syntax will be presented in the subsequent content.

Single System	
Remote In-Band	<code>./saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS user ID&gt; --os_key &lt;OS private key&gt; --os_key_pw &lt;OS private key password&gt; -c &lt;command&gt; [command options]</code>

#### 4.3.4.3. Using Remote Redfish Host Interface (Remote\_RHI)

Syntax:

Single System	
Remote In-Band	<code>./saa -I Remote_RHI -u &lt;username&gt; -p &lt;password&gt; --oi &lt;OS IP address&gt; --ou &lt;OS user ID&gt; --op &lt;OS user password&gt; -c &lt;command&gt; [command options]</code>

---

For commands or managed systems that require the use of Redfish Host Interface (see 4.3.3 Redfish Host Interface), both the BMC and OS username and password of the remote system are needed.

Alternatively, you can use the `--os_key` and `--os_key_pw` options to log in to a remote system through a private key. For simplicity, only the first syntax will be presented in the subsequent content.

Single System	
Remote In-Band	<code>./saa -I Remote_RHI -u &lt;username&gt; -p &lt;password&gt; --oi &lt;OS IP address&gt; --ou &lt;OS user ID&gt; --os_key &lt;OS private key&gt; --os_key_pw &lt;OS private key password&gt; -c &lt;command&gt; [command options]</code>

#### 4.3.4.4. Console Output

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

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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.
```

#### 4.3.4.5. Supported Commands

Currently, the available commands for this usage include:

##### BIOS Management:

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

---

### BMC Management:

GetBmcInfo, UpdateBmc, GetBmcCfg, ChangeBmcCfg, GetBmcLANCfg, ChangeBmcLANCfg, SetBmcPassword, GetKcsPriv, GetLockdownMode, LoadDefaultBmcCfg, TimedBmcReset, GetBmcUserList, SetBmcUserList, BmcHostName

### Applications:

RemoteExec

Example:

#### **Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c RemoteExec --remote_cmd "ls ~/supermicro/saa_remote_inband/ -l | grep
test.sh" --file test.sh
```

#### **Remote In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p Password --oi 192.168.34.57 -
-ou root --op 111111 -c GetBmcInfo --remote_saa /root/saa
```

#### **4.3.4.6. Transferring Files**

When executing Remote In-Band commands that involve a file transfer, SAA creates a new file (randomly named by 8 characters) in the saa\_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 saa.log file is also created. See 4.6 SAA Logs 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.

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c <command> --file <file> --remote_saa /root/saa
```

**The console output contains the following information:**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
```

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

```
Sending file 'sample.txt' to '/root/saa_remote_inband/2022-11-18_14-09-58/sample.txt' on 192.168.34.56.
```

```
=====
```

```
Console Output from the Remote Managed System 192.168.34.56
```

```
=====
```

```
Getting file 'sample.txt' from '/root/saa_remote_inband/2022-11-18_14-09-58/sample.txt' on 192.168.34.56.
```

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

## 4.4. Managing Multiple Systems

For managing multiple systems, SAA provides the “-l” option to concurrently execute commands on multiple systems enumerated in a system list file.

When managing a large number of systems, the option “--batch\_count” divides the systems in the list into multiple batches for execution, and each batch will have a separate log file.

Multiple Systems	
OOB	saa -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:

```
[SAA_HOME]# ./saa -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 192.168.34.56, SAA applies -u ADMIN and -p PASSWORD to the command line to execute the GetDmiInfo command. For the second managed system 192.168.34.57, SAA adopts the username (ADMIN1) and password (PASSWORD1) in SList.txt to execute the GetDmiInfo command.

Multiple Systems	
Remote In-Band	saa {-l Remote_INB   -l Remote_RHI} -l <system list file> -c <command> [command options] [--remote_saa <remote SAA path>]

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:

```
[SAA_HOME]# ./saa {-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\_INB:

```
192.168.34.56 root 111111
192.168.34.57 root /root/pvt_key 111111 ADMIN PASSWORD1
```

Two executions are run concurrently and the execution status/results can be referenced in >4.4.1.2 File Output, 4.4.1.3 Screen Output and 4.4.1.4 Log Output.

For the use of commands that take input files as arguments, such as the UpdateBios command, see 4.4.1.1 File Input for its usage.



**Notes:**

- For the ActivateProductKey command, different formats are used. Refer to 5.3.1 Activating the Node Product Keys.
  - For the SetBiosPassword command, different formats are used. Refer to 5.6.11 Setting Up a BIOS Administrator Password.
  - For the RemoteExec command, different formats are used. Refer to 5.13.8 Remote Execution.
  - For the CpuOnDemand command, different formats are used. Refer to 5.3.3 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.
  - SAA limits its maximum concurrent execution count to avoid system overloading. The default thread\_count in the .saarc file is 50. For more details on usages, see 4.2 Customizing SAA Configurations
-

---

## 4.4.1. Input Output Controls for Multiple Systems

### 4.4.1.1. File Input

SAA uses the input file specified in the command line (through --file option) to manage multiple systems.

Example:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateBios --file Supermicro_BIOS.bin
```

SList.txt:

```
192.168.34.56
192.168.34.57
```

In this example, SAA uses the input file Supermicro\_BIOS.bin 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:**

SAA only supports single input files for managed systems in one command.

---

### 4.4.1.2. File Output

When SAA 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:

```
[SAA_HOME]# ./saa -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.

#### 4.4.1.3. Screen Output

When SAA begins the execution for the managed systems, progress output will be continuously updated to a log file created when SAA is invoked.

When the SAA finishes execution, the final execution status for each managed system will be shown on the screen output row-by-row. Each row consists of “Index”, “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,” “SUCCESS,” “FAILED,” “INCOMPLETE,” “RETRY,” “IGNORED,” or “CANCEL.” The status summary will be shown before and after the status list. After listing the final status, SAA 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.

When managing a large number of systems in batches using the --batch\_count option, the final result on the screen output will only show the status summary and log name of each batch. For the final status of individual systems, please refer to the contents of *4.4.1.4. Log Output*.

Example:

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt --show_multi_full
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt --batch_count
```

```
SList.txt:
192.168.34.56
192.168.34.57
192.168.34.58
```

### Screen Output:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt
```

```
SuperServer Automation Assistant 1.0.0 (2024/03/06) (x86_64)
Copyright(C) 2024 Super Micro Computer, Inc. All rights reserved.
The average upload speed per thread is limited to 333 mbps on higher bandwidth
system, while the speed is limited to 2 mbps on lower bandwidth system.
Start to do GetDmiInfo for systems listed in SList.txt

Multi system log file created:
 SList.txt.log_2024-03-06_15-50-43_5228
Press ENTER to see the current execution (Index: 1 ~ 3) status:

-----Current Status-----
Executed Command:
 ./saa -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt
Summary:
 3 EXECUTIONS (WAITING: 0 RUNNING: 2 SUCCESS: 1 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)
Status List:
 Index | System Name | Elapsed | Status | Exit Code
 2 | 192.168.34.57 | 00:00:03 | RUNNING |
 3 | 192.168.34.58 | 00:00:03 | RUNNING |
Summary:
 3 EXECUTIONS (WAITING: 0 RUNNING: 2 SUCCESS: 1 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)

-----Final Results-----
```

Executed Command:

```
./saa -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt
```

Summary:

```
3 EXECUTIONS (WAITING: 0 RUNNING: 0 SUCCESS: 3 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)
```

Status List:

Index	System Name	Elapsed	Status	Exit Code
1	192.168.34.56	00:00:03	SUCCESS	0
2	192.168.34.57	00:00:05	SUCCESS	0
3	192.168.34.58	00:00:05	SUCCESS	0

Summary:

```
3 EXECUTIONS (WAITING: 0 RUNNING: 0 SUCCESS: 3 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)
```

Please check output message:

SList.txt.log\_2024-03-06\_15-50-43\_5228

```
[SAA_HOME]#./saa -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file
DMI.txt --show_multi_full
```

SuperServer Automation Assistant 1.0.0 (2024/03/06) (x86\_64)

Copyright(C) 2024 Super Micro Computer, Inc. All rights reserved.

The average upload speed per thread is limited to 333 mbps on higher bandwidth system, while the speed is limited to 2 mbps on lower bandwidth system.

Start to do GetDmiInfo for systems listed in SList.txt

Multi system log file created:

SList.txt.log\_2024-03-06\_15-56-06\_6563

Press ENTER to see the current execution (Index: 1 ~ 3) status:

-----Current Status-----

Executed Command:

```
./saa -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt
```

--show\_multi\_full

Summary:

```
3 EXECUTIONS (WAITING: 0 RUNNING: 2 SUCCESS: 1 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)
```

Status List:

Index	System Name	Elapsed	Status	Exit Code
1	192.168.34.56	00:00:02	SUCCESS	0
2	192.168.34.57	00:00:03	RUNNING	
3	192.168.34.58	00:00:03	RUNNING	

Summary:

```
3 EXECUTIONS (WAITING: 0 RUNNING: 2 SUCCESS: 1 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)
```

-----Final Results-----

Executed Command:

```

./saa -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt
--show_multi_full
Summary:
 3 EXECUTIONS (WAITING: 0 RUNNING: 0 SUCCESS: 3 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)
Status List:
 Index | System Name | Elapsed | Status | Exit Code
 1 | 192.168.34.56 | 00:00:02 | SUCCESS | 0
 2 | 192.168.34.57 | 00:00:02 | SUCCESS | 0
 3 | 192.168.34.58 | 00:00:02 | SUCCESS | 0
Summary:
 3 EXECUTIONS (WAITING: 0 RUNNING: 0 SUCCESS: 3 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)

Please check output message:
SList.txt.log_2024-03-06_15-56-06_4392

```

[SAA\_HOME]#/saa -l SList.txt -u ADMIN -p PASSWORD -c GetDmiInfo --file DMI.txt --batch\_count

```

SuperServer Automation Assistant 1.0.0 (2024/03/06) (x86_64)
Copyright(C) 2024 Super Micro Computer, Inc. All rights reserved.
The average upload speed per thread is limited to 333 mbps on higher bandwidth
system, while the speed is limited to 2 mbps on lower bandwidth system.
Start to do GetDmiInfo for systems listed in SList.txt

Multi system log file created:
 SList.txt.log_2024-03-06_15-56-06_6563_1
Press ENTER to see the current execution (Index: 1 ~ 2) status:

Multi system log file created:
 SList.txt.log_2024-03-06_15-56-06_6563_2
Press ENTER to see the current execution (Index: 3 ~ 3) status:

-----Current Status-----
Executed Command:
 ./saa -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt
--batch_count 2
Summary:
 1 EXECUTIONS (WAITING: 0 RUNNING: 1 SUCCESS: 0 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)
Status List:
 Index | System Name | Elapsed | Status | Exit Code
 3 | 192.168.34.58 | 00:00:03 | RUNNING |
Summary:
 1 EXECUTIONS (WAITING: 0 RUNNING: 1 SUCCESS: 0 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)

-----Final Results-----

```

```

Executed Command:
./saa -u ***** -p ***** -l SList.txt -c GetDmiInfo --file DMI.txt
--batch_count 2
Summary (SList.txt.log_2024-03-06_15-56-06_6563_1):
 2 EXECUTIONS (WAITING: 0 RUNNING: 0 SUCCESS: 2 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)
Summary (SList.txt.log_2024-03-06_15-56-06_6563_2):
 1 EXECUTIONS (WAITING: 0 RUNNING: 0 SUCCESS: 1 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)

```

#### 4.4.1.4. Log Output

When SAA is executed for the managed systems, a log file is created and continuously updated with execution messages for each system. The log file name, which will be shown on screen, is the system list file name appended by ".log\_," "yyyy-mm-dd\_hh-mm-ss" (date and time), "\_PID' (process ID)," and "\_logNumber" (if the --batch\_count option is entered.). 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 dedicated system output. The following example shows the log file SList.txt.log\_2023-10-02\_15:57:40\_7370 created from the example in 4.4.1.3 *Screen Output*.

The SList.log will be saved in /var/log/supermicro/SAA if it exists. Otherwise, it will be saved in the same folder as SList.txt.

Example:

```

-----Last Update Time-----
2024-03-06_15:57:47
Process finished.
-----Execution parameters-----
Executed Command:
./saa -l SList.txt -u ADMIN -p ***** -c GetDmiInfo --file DMI.txt

-----Summary-----
 2 EXECUTIONS (WAITING: 0 RUNNING: 0 SUCCESS: 2 FAILED: 0 INCOMPLETE: 0
RETRY: 0 IGNORED: 0 CANCEL: 0)

-----Status List-----
Index |System Name |Start Time |End Time |Elapsed |Status |
|Exit Code
1 |192.168.34.56 |10-02_15:57:40 |10-02_15:57:42 |00:00:02|SUCCESS |0
2 |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
SuperServer Automation Assistant 1.0.0 (2024/03/06) (x86_64)
Copyright(C) 2024 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
SuperServer Automation Assistant 1.0.0 (2024/03/06) (x86_64)
Copyright(C) 2024 Super Micro Computer, Inc. All rights reserved.

File "DMI.txt.192.168.34.57" is created.

```

## 4.5. Command Options

### 4.5.1. License Management

License Management	
Commands	Long Options
ActivateProductKey	<b>--key &lt;node product key value&gt; (Optional)</b> Uses the node product key to activate the managed system.  <b>--key_file &lt;file name&gt; (Optional)</b> Uses the node product key file to activate the managed system.
QueryProductKey	<b>--show_index (Optional)</b> Prints the key index information.  <b>--showall (Optional)</b> Prints the key index and full key information.
CpuOnDemand	<b>--action</b> 1 = GetHwInfo 2 = GetOnDemandState 3 = SetLicenseActivateCode 4 = EnablePPIN  <b>-v</b> Prints extra info of CAP and registers in action 2 = GetOnDemandState.

	<p><b>--cpu_id &lt;CPU ID&gt;</b> CPU ID to indicate CPU socket.</p> <p><b>--hw_id &lt;Hardware ID&gt;</b> Hardware ID to indicate the PPIN of the CPU socket.</p> <p><b>--hw_id_file &lt;Hardware ID file&gt;</b> Hardware ID file with the format of "BMC MAC;CPU ID;PPIN".</p> <p><b>--lac_file &lt;LAC+ map file&gt;</b> License file in the format of "PPIN;LAC+(s)" used in action 3 = SetLicenseActivateCode.</p> <p><b>--cfg_file &lt;SDSi-agent config file&gt;</b> SDSi-agent config file, only useful in action 2 = GetOnDemandState and specifying -v.</p> <p><b>--skip_gap &lt;Skip gap(s)&gt;</b> Skips the gap of LAC revision ID and continues provisioning.</p> <p><b>--squash &lt;Squash into one file&gt;</b> Squashes the state reports into one file in the format of "PPIN;State Report."</p> <p><b>--plain_text &lt;Output state as plain text&gt;</b> Prints the on-demand state as plain text.</p> <p><b>--file &lt;file name&gt;</b> Save to file in action 1 = GetHwInfo and action 2 = GetOnDemandState or provide license file in action 3 = SetLicenseActivateCode.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system POST to complete after rebooting.</p> <p><b>--overwrite (Optional)</b> Overwrites the hardware ID or on-demand state report file.</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 4.5.2. Health Management

Health Check	
Commands	Long Options
CheckOOBSupport	None

CheckAssetInfo ( <b>OOB only</b> )	None
CheckSensorData ( <b>OOB only</b> )	<p><b>--action (Optional)</b>  1 = Show  2 = Del  3 = GetVer  4 = SetVer</p> <p><b>--sdr_id (Optional)</b>  The SDR ID for delete.</p> <p><b>--sdr_major_version (Optional)</b>  The SDR major version.</p> <p><b>--sdr_minor_version (Optional)</b>  The SDR minor version.</p> <p><b>--showall (Optional)</b>  Shows the IPMI sensor all threshold values of the managed system.</p>
CheckSystemUtilization ( <b>OOB only</b> ) (TAS thin agent is required.)	None
ServiceCalls	<p><b>--file &lt;file name&gt;</b>  Monitors the host with the given XML-style file listing system event logs and sensor data records to be monitored.</p>
SystemPFA	<p><b>--action</b>  1 = GetCurrentStatus  2 = Enabled  3 = Disabled</p> <p><b>--reboot (Optional)</b>  Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b>  Waits for the managed system's POST to complete after rebooting.</p>
MemoryHealthCheck	<p><b>--action</b>  1 = GetCurrentStatus  2 = Persistent  3 = Enable</p>

	<p>4 = Disable</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system POST to complete after rebooting.</p>
ChassisIntrusion	<p><b>--action</b> 1 = Status 2 = Clear</p>
AlertManage	<p><b>--action &lt;action&gt;</b> 1 = listMessage 2 = sendTest</p> <p><b>--message_type &lt;List of message type&gt;</b> 1 = nmpv1 3 = snmpv3 4 = redfishAlert</p> <p><b>--after &lt;datetime&gt;(Optional)</b> Queries trap messages after specified time</p> <p><b>--before &lt;datetime&gt;(Optional)</b> Queries trap messages before specified time</p> <p><b>--ip &lt;Sender IP&gt;(Optional)</b> Queries trap message of the specified IP address</p> <p><b>--page &lt;Page&gt;(Optional)</b> Sets Page number and the default value is first page</p> <p><b>--limit &lt;limit&gt;(Optional)</b> Sets quantity of data with one page, and range is 10 to 100, the default value is twenty</p>
SuperDiag	<p><b>--action &lt;action&gt;</b> Sets SuperDiag action to: 1 = Start 2 = Download 3 = Display 4 = List</p> <p><b>--file &lt;file name&gt;(Optional)</b> Start action: Mounts the ISO image to run diagnostics. Download/Display action: Enters the filename for diagnostic results.</p>

	<p><b>--image_url &lt;URL&gt;(Optional)</b>  The URL to access the shared ISO image file. URL format:  'http://&lt;IPv4 or IPv6&gt;/&lt;shared point&gt;/&lt;file path&gt;' or  'https://&lt;IPv4 or IPv6&gt;/&lt;shared point&gt;/&lt;file path&gt;'</p> <p><b>--dev_id &lt;Device ID&gt;(Optional)</b>  The specified device to mount ISO image.  The supported device ID: [1-3]</p> <p><b>--overwrite (Optional)</b>  Overwrites the diagnostic results file.</p> <p><b>--reboot (Optional)</b>  Forces the managed system to reboot or power up after operation.</p> <p><b>--type &lt;type&gt;(Optional)</b>  Set display type to:  0 = Info  1 = Pass  2 = Fail</p> <p>(The input type string will be converted to the above type number)</p> <p><b>--line &lt;number&gt;(Optional)</b>  Prints the number of lines at a time.</p> <p><b>--type &lt;type&gt;(Optional)</b>  Prints results that match the keyword.</p> <p><b>--usb (Optional)</b>  For action Start: Starts a diagnostic with local USB device.  For action List: Lists available device indexes to mount local USB.</p> <p><b>--index &lt;index&gt;(Optional)</b>  The specified index to mount local USB.</p>
SendDiagInterrupt	None
MonitorCDUStatus	<p><b>--file &lt;file name&gt;(Optional)</b>  For action 1 = GetStatus  Prints the status on screen if the file-saving function is not available.  For action 2 = SetCfg  Sets the CDU Alert option.</p>

	<p>Monitors the host with the given JSON file listing device and sensor data records to be monitored.</p> <p><b>--action</b> Sets CDU action with: 1 = GetStatus 2 = SetCfg</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p>
<p>TasManage</p> <p>(TAS thin agent is required.)</p>	<p><b>--action</b> Sets TAS action with: GetInfo Pause Resume Refresh Clear SetPeriod</p> <p><b>--period (Optional)</b> Sets the TAS update period in seconds (between 5 and 60).</p>
CheckSelfTest	None
HDTService	<p><b>--action</b> 1 = GetCurrentStatus 2 = Enable 3 = Disable</p>

### 4.5.3. System Management

System Management	
Commands	Long Options
GetFruInfo	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the dumped FRU data to a file.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p> <p><b>--showall (Optional)</b> Gets all FRU information from managed system. Gets all FRU info from the managed system.</p> <p><b>--file_only (Optional)</b> Works with the --file option and only reads FRU information from</p>

	<p>the input dumped FRU binary file.</p> <p><b>--dump (Optional)</b> Works with the --file option and dumps FRU data.</p> <p><b>--format &lt;file format&gt; (Optional)</b> Works with the --file and --dump options to download FRU data to file in one of the following specified formats: BINARY = Binary format TEXT = Text format If the --format option is not provided, the default format is BINARY.</p> <p><b>--dev_id &lt;Device ID&gt;(Optional)</b> 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) 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</p>
RestoreFruInfo	<p><b>--file &lt;file name&gt;</b> Reads the dumped FRU file.</p> <p><b>--format &lt;file format&gt; (Optional)</b> Works with the --file option to read a FRU file in one of the following specified formats: BINARY = Binary format TEXT = Text format If the --format option is not provided, the default format is BINARY.</p> <p><b>--individually (Optional)</b> Restores each BMC with the corresponding FRU info file individually.</p>

ChangeFruInfo	<p><b>--item &lt;item name&gt;</b> Updates the FRU information with given FRU field.  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  ALL = All Fields</p> <p><b>--value &lt;assignment value&gt;</b> Updates the value of the given FRU field.  If the item is ALL, the format is  "&lt;CT&gt;,&lt;CP&gt;,&lt;CS&gt;,&lt;BDT&gt;,&lt;BM&gt;,&lt;BPN&gt;,&lt;BS&gt;,&lt;BP&gt;,&lt;PM&gt;,&lt;PN&gt;,&lt;PPM&gt;,&lt;PV&gt;,&lt;PS&gt;,&lt;PAT&gt;"</p> <p><b>--fru_version &lt;FRU version&gt;</b> Updates the FRU version.</p>
GetSystemInfo	None
GetSystemCfg	<p><b>--file &lt;file name&gt;</b> Saves the configuration to a file.</p> <p><b>--current_password &lt;current password&gt;</b> Checks the current BIOS Administrator password.</p> <p><b>--download</b> Downloads the current Blade system configuration file accessible for profile update from the CMM.</p> <p><b>--file_id &lt;file ID&gt;</b> Downloads the existing Blade system profile from the CMM with the specific file ID.</p> <p><b>--overwrite</b> Overwrites the output file.</p> <p><b>--dev_id &lt;Device ID&gt;</b> Assigns Blade index and node ID.  Blade index: [A1-A14] or [B1-B14]  Node ID: [1-4]  Format: [A1_1]</p>



	<p><b>--cur_pw_file &lt;Current password file&gt;</b> The specified file path to read BIOS Administrator password.</p> <p><b>--action</b> Sets the action offer for each XML table. Acceptable options: None or Change.</p>
ChangeSystemCfg	<p><b>--file &lt;file name&gt;</b> Updates the managed system with the given configuration file.</p> <p><b>--current_password &lt;current password&gt;</b> Checks the current BIOS Administrator password.</p> <p><b>--upload</b> Uploads the Blade system configuration file to the CMM for updating profile.</p> <p><b>--file_id &lt;file ID&gt;</b> Assigns the profile ID using the ProfileManage command.</p> <p><b>--update &lt;update rule&gt;</b> Updates the Blade system configurations with the existing system profile on the CMM. Supported update rules: [Apply] or [Deploy]</p> <p><b>--skip_precheck (Optional)</b> Uploads and overwrites the existing CMM profile.</p> <p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--dev_id &lt;Device ID&gt;</b> Assigns Blade index and node ID. Blade index: [A1-A14] or [B1-B14] Node ID: [1-4] Format: [A1], [A1_1] or [ALL] for all blade nodes</p> <p><b>--skip_unknown</b> Skips the unknown settings or menus in the system configuration file.</p> <p><b>--skip_bbs</b> Skips the BBS-related menus in the BIOS configuration file.</p> <p><b>--precheck</b> Checks the configuration before the update.</p> <p><b>--post_complete</b> Waits for the managed system's to POST complete after</p>

	rebooting.  <b>--cur_pw_file &lt;Current password file&gt;</b> The specified file path to read BIOS Administrator password.
GetFanMode	None
SetFanMode	<b>--fanmode &lt;Fan Mode Type&gt;</b> Sets the fan mode to the following options: 0 = Standard 1 = Full 2 = Optimal 3 = PUE2 Optimal 4 = Heavy IO 5 = PUE3 Optimal 6 = Liquid Cooling 7 = Smart Cooling  (The input type string will be converted to the above type number)
LocateServerUid	<b>--action &lt;action&gt;</b> Sets action to: 1 = GetStatus 2 = On 3 = Off
GetFirmwareInventoryInfo	<b>--json_view (Optional)</b> Show the Firmware Inventory info in json formats.
ClearCMOS	<b>--ac_cycle</b> Proceeds to AC cycle the managed system after the operation.

#### 4.5.4. BIOS Management

BIOS Management	
Commands	Long Options
UpdateBios	<b>--file &lt;file name&gt;</b> Updates the BIOS with the given BIOS image file.  <b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.

---

**--individually (Optional)**

Individually updates each BIOS with its corresponding image file.

**--flash\_smbios (Optional)**

Overwrites and resets the SMBIOS data. This option is used only for specific purposes. Unless you are familiar with SMBIOS data, do not use this option.

**--preserve\_nv (Optional)**

Preserves the NVRAM. This option is used only for specific purposes. Unless you are familiar with BIOS NVRAM, do not use this option. (Not available on X12 and later systems.)

**--preserve\_mer (Optional)**

Preserves the ME firmware region. This option is used only for specific purposes. Unless you are familiar with ME firmware image, do not use this option. (Not available on X12 and later RoT systems.)

**--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.

**--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.

	<p><b>--restore_optimized_default (Optional)</b> Restores the BIOS configurations to optimized default settings.</p> <p><b>--redfish (Optional)</b> Enables support for pure Redfish.</p>
GetBiosInfo	<p><b>--file &lt;file name&gt; (Optional)</b> Reads BIOS information from an input BIOS image file.</p> <p><b>--individually (Optional)</b> Gets each BIOS with its corresponding image file individually.</p> <p><b>--showall (Optional)</b> Prints the BIOS version, BIOS revision and BIOS OEM FID information.</p> <p><b>--file_only (Optional)</b> Works with --file, and only reads BIOS information from the input image file.</p> <p><b>--extract_measurement (Optional)</b> Works with --file, extract BIOS image file measurement.</p> <p><b>--showall(Optional)</b> Prints the last BMC reset time.</p> <p><b>--redfish (Optional)</b> Enables support for pure Redfish.</p>
GetDefaultBiosCfg	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the BIOS configuration to a file. Prints the default factory BIOS configuration on the screen if the file-saving function is not available.</p> <p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p>
GetCurrentBiosCfg	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the BIOS configuration to a file. Prints the current BIOS configuration on the screen if the file-saving</p>

	<p>function is not available.</p> <p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p> <p><b>--tui (Optional)</b> Edits the BIOS configuration with text-based user interface.</p> <p><b>--compact (Optional)</b> Generates a compact version of the BIOS configuration containing only the settings that have been changed in the text-based user interface.</p>
ChangeBiosCfg	<p><b>--file &lt;file name&gt; (Optional)</b> Updates the BIOS with the given configuration file.</p> <p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--individually (Optional)</b> Updates each BIOS individually with the corresponding configuration file.</p> <p><b>--skip_unknown (Optional)</b> Skips the unknown settings or menus in the BIOS configuration file.</p> <p><b>--skip_bbs (Optional)</b> Skips the BBS-related menus in the BIOS configuration file.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p> <p><b>--save_as_user_default (Optional)</b> Saves the current BIOS configuration as user default.</p>

LoadDefaultBiosCfg	<p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p> <p><b>--clear_bios_eventlog (Optional)</b> Clears the BIOS event log.</p> <p><b>--optimized_default (Optional)</b> Restores the BIOS to default settings with optimization.</p> <p><b>--show (Optional)</b> Shows the BIOS current default status.</p>
GetDmiInfo	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the DMI information to a file. Prints the DMI information on the screen if the file-saving function is not available.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p>
EditDmiInfo	<p><b>--file &lt;file name&gt;</b> The DMI information file to be edited (or created if it does not exist).</p> <p><b>--item_type &lt;item type&gt;</b> Specifies the item type.</p> <p><b>--item_name &lt;item name&gt;</b> Specifies the item name.</p> <p><b>--shn &lt;short name&gt;</b> Specifies the item in short name format.</p> <p><b>--value &lt;assignment value&gt;</b> Assigns the value to the item.</p> <p><b>--default</b> Assigns the default value to the item.</p> <p><b>Notes:</b></p>

	<ul style="list-style-type: none"> <li>• Either [--item_type, --item_name] or [--shn] is required.</li> <li>• Either [--value] or [--default] is required.</li> </ul>
ChangeDmiInfo	<p><b>--file &lt;file name&gt;</b> Updates the DMI information with the given text file.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--individually (Optional)</b> Individually updates each piece of DMI information with its corresponding text file.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
SetBiosPassword	<p><b>--new_password &lt;new password&gt; (Optional)</b> Sets the new BIOS Administrator password.</p> <p><b>--confirm_password &lt;confirm password&gt; (Optional)</b> Confirms the new BIOS Administrator password.</p> <p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--pw_file &lt;Password File&gt; (Optional)</b> The specified file path to read the new password.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p>
EraseOAKey (In-band Only)	<p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p>
GetScplInfo	<p><b>--file_only</b> Works with the --file option, and only reads SCP information from the input image file.</p>

UpdateScp	<p><b>--file &lt;file name&gt;</b> Updates the SCP with the given SCP image file.</p> <p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--individually (Optional)</b> Updates each SCP with its corresponding firmware file individually.</p>
GetFixedBootCfg	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the configuration to a file. Prints the BIOS fixed boot order configuration on screen if the file-saving function is not available.</p> <p><b>--redfish</b> Gets the BIOS fixed boot order with the pure Redfish solution.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p>
GetBootOption	None
SetBootOption	<p><b>--device_type &lt;Device Type ID&gt;</b> 0: No Override</p> <p>Sets the Device_Type to the following numbers for Legacy Device:</p> <ul style="list-style-type: none"> <li>1: PXE</li> <li>2: Hard Drive</li> <li>3: CD DVD</li> <li>4: BIOS Setup</li> <li>5: USB Key</li> <li>6: Virtual USB Hard Drive</li> <li>7: Virtual Floppy</li> <li>8: ISO Image</li> </ul> <p>Sets the Device_Type to the following numbers for UEFI Device:</p> <ul style="list-style-type: none"> <li>9: UEFI: Hard Drive</li> <li>10: UEFI: CD DVD</li> <li>11: UEFI: USB Key</li> <li>12: Virtual UEFI: USB Hard Drive</li> <li>13: UEFI: ISO Image</li> <li>14: UEFI: PXE</li> <li>15: UEFI: Floppy Virtual Floppy</li> <li>16: UEFI: BIOS Shell</li> </ul> <p><b>--action &lt;action&gt; (Optional)</b> Sets power action with:</p>



	<p>0 = up 1 = down 2 = cycle 3 = reset 4 = softshutdown 5 = reboot</p> <p><b>--post_complete (Optional)</b> Waits for the managed system POST complete after rebooting.</p> <p><b>--next_boot_only &lt;Enable/Disable&gt; (Optional)</b> Sets NextBootOnly status to Enable/Disable The default value is Enable</p> <p><b>--bypass_password &lt;Enable/Disable&gt;</b> Sets ByPassWord status to Enable/Disable The default value is Disable</p>
SetHttpBoot	<p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read current password.</p> <p><b>--file &lt;file name&gt;</b> Uploads the TLS certificate in the formats of .cer, .der, .crt, or .pem.</p> <p><b>--boot_name &lt;boot description&gt;</b> Description for HTTP boot.</p> <p><b>--boot_lan &lt;boot lan port&gt;</b> Enters the LAN port for HTTP boot.</p> <p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--boot_clean</b> Cleans all HTTP boot options.</p> <p><b>--disable_hostname_check</b> Disables checking whether the host name of the TLS certificate matches the host name provided by the remote server for HTTPS boot.</p> <p><b>--image_url &lt;URL&gt;</b> The URL to access the shared image file. URL format: 'http://&lt;IPv4 or IPv6&gt;/&lt;shared point&gt;/&lt;file path&gt;' or 'https://&lt;IPv4 or IPv6&gt;/&lt;shared point&gt;/&lt;file path&gt;'</p>

	<b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.
ChangeFixedBootCfg	<b>--file &lt;file name&gt;</b> Updates the BIOS fixed boot order with the given configuration file.  <b>--redfish</b> Updates the BIOS fixed boot order with the pure Redfish solution.  <b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.  <b>--individually (Optional)</b> Updates each fixed BIOS boot configuration with the corresponding configuration file individually.  <b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.
GetBiosPostCode	<b>--redfish</b> Uses the Redfish Host Interface for in-band get BIOS POST code. (Only in-band usage is supported.)

### 4.5.5. BMC Management

BMC Management	
Commands	Long Options
UpdateBmc	<b>--file &lt;file name&gt;</b> Updates the BMC with the given BMC file.  <b>--individually (Optional)</b> Updates each BMC with its corresponding image file individually.  <b>--overwrite_cfg (Optional)</b> Overwrites the current BMC configuration using the factory default values in the given BMC image file.  <b>--overwrite_sdr (Optional)</b> Overwrites current BMC SDR data. For AMI BMC FW, it must use the --overwrite_cfg option as well.  <b>--overwrite_ssl (Optional)</b> Overwrites current BMC SSL configuration.

	<p><b>--backup (Optional)</b> Backs up the current BMC image. (Only supported by the RoT systems.)</p> <p><b>--forward (Optional)</b> Confirms the Rollback ID and upgrades to the next revision.</p> <p><b>--bmc_boot_check (Optional)</b> Checks if BMC boots up within 16 minutes after update. (Only supported on X12/H12 and later platforms except the H12 non-RoT systems.)</p> <p><b>--redfish (Optional)</b> Enables support for pure Redfish</p>
GetBmcInfo	<p><b>--file &lt;file name&gt; (Optional)</b> Reads the BMC information from the input BMC image file.</p> <p><b>--individually (Optional)</b> Gets information of BMC on each system with the corresponding configuration file individually.</p> <p><b>--file_only (Optional)</b> Works with --file option, and only reads BMC information from the input image file.</p> <p><b>--extract_measurement (Optional)</b> Works with the --file option, and extracts BMC image file measurement.</p> <p><b>showall</b> Works with the --showall option to display all information.</p>
GetBmcCfg	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the configuration to a file. Prints the BMC configuration on screen if the file-saving function is not available.</p> <p><b>--dump (Optional)</b> Dumps read-only BMC configuration file.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p> <p><b>--sample_file(Optional)</b> Creates BMC configuration using the format from the sample file.</p>

	<p><b>--action(Optional)</b> Sets the action of each XML table. Acceptable option: None or Change.</p>
ChangeBmcCfg	<p><b>--file &lt;file name&gt;</b> Updates the BMC with the given configuration file.</p> <p><b>--restore (Optional)</b> Restores the BMC configuration with the corresponding read-only configuration file.</p> <p><b>--individually (Optional)</b> Updates each BMC with the corresponding configuration file individually.</p> <p><b>--skip_unknown (Optional)</b> Skips the unknown tables or settings in the BMC configuration file.</p>
SetBmcPassword	<p><b>--user_id &lt;user ID&gt;</b> Enters the BMC user ID.</p> <p><b>--new_password &lt;new password&gt;</b> Sets the new BMC user password.</p> <p><b>--confirm_password &lt;confirms password&gt;</b> Confirms the new BMC user password.</p> <p><b>--pw_file &lt;password file&gt;</b> The specified file path to read the new BMC user password.</p>
GetKcsPriv	None
SetKcsPriv (OOB Only)	<p><b>--priv_level &lt;KCS privilege level&gt;</b> Sets KCS privilege with level. 1 = Call Back 2 = User 3 = Operator 4 = Administrator</p>
LoadDefaultBmcCfg	<p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--redfish (Optional)</b> Enables support for pure Redfish.</p>

	<p><b>--clear_user_cfg (Optional)</b> Clears user configuration.</p> <p><b>--preserve_user_cfg (Optional)</b> Preserves user configuration.</p> <p><b>--load_unique_password (Optional)</b> Loads the unique BMC password.</p> <p><b>--load_default_password (Optional)</b> Loads the default BMC password.</p> <p><b>--load_default_lan (Optional)</b> Loads the default BMC LAN configuration.</p> <p><b>--load_default_fru (Optional)</b> Loads the default FRU configuration.</p> <p><b>--bmc_boot_check (Optional)</b> Check if BMC is booted up after reset.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system POST complete after rebooting.</p>
TimedBmcReset	<p><b>--immediate &lt;immediately&gt;(Optional)</b> Resets BMC immediately.</p> <p><b>--delay &lt;BMC reset delay time&gt; (Optional)</b> Delay reset time. Note: Delay time must be set to 1 to 60 minutes.</p> <p><b>--bmc_boot_check (Optional)</b> Checks BMC boots up within 4 minutes after reset.</p>
GetBmcUserList	None
SetBmcUserList	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = Add 2 = Del 3 = Level 4 = SetPwd 5 = Test 6 = EnableType 7 = EnableAccount 8 = EditUserName</p>

---

**--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

The "Callback" privilege level is not supported on open BMC system.

The "No Access" privilege level is not supported.

**--user\_status <user enable> (Optional)**

Manages the status of a BMC user.

0 = Disable

1 = Enable

**--account\_type <account type> (Optional)**

Supported account types for BMC management.

0 = SNMP

**--account\_type\_status <account type status> (Optional)**

Manage account type status.

0 = Disable

1 = Enable

**--ap <authentication protocol> (Optional)**

The authentication protocol.

0 = MD5

1 = SHA

**--pp <private protocol> (Optional)**

The authentication protocol.

0 = DES

1 = AES

**--ak <authentication key> (Optional)**

The authentication key.

**--pk <private key> (Optional)**

The private key.

**--manage\_account\_type <manage account type> (Optional)**

Manages the status of account types.

	<p>The format is "SNMP:Enable,Redfish:Disable." Supported account types are:</p> <ol style="list-style-type: none"> <li>1. Redfish</li> <li>2. SNMP</li> </ol>
BootStrappingAccount	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = CreateAccount 2 = DeleteAccount 3 = CheckAccount</p> <p><b>--user_name &lt;user name&gt; (Optional)</b> Deletes a bootstrapping account with a user name.</p>
RmcpManage	<p><b>--action &lt;action&gt;</b> Sets RMCP status with: 1 = GetInfo 2 = Enable 3 = Disable</p> <p><b>--port &lt;port&gt; (Optional)</b> Command optional port(s). The format of &lt;port&gt; is "RMCP:623" or "623". List of optional port(s) for the command : 1.RMCP (for RMCP service port)</p>
BmcHostName	<p><b>--action &lt;action&gt;</b> Sets RMCP status with: 1 = Get 2 = Set</p> <p><b>--hostname &lt;Host Name&gt; (Optional)</b> Host name</p>
ManageRHI	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = GetConnection 2 = SetConnection</p> <p><b>--type &lt;type&gt; (Optional)</b> Sets USB connection Supported connection type string: 0 = RNDIS</p>

	1 = CDC_ECM (The input type string will be converted to the above type number.)
BmcWatchdog	<p><b>--action &lt;action&gt;</b>          Sets WatchDog actions to:          0 = Set          1 = Info          2 = Reset</p> <p><b>--timer_action &lt;Watchdog timer actions&gt;</b>          Sets WatchDog timer actions to:          0 = NoAction          1 = HardReset          2 = PowerDown          3 = PowerCycle</p> <p><b>--interval &lt;time interval&gt;</b>          Sets WatchDog pre-timeout interval in seconds.</p>
snmpManage	<p><b>--action &lt;action&gt;</b>          Sets action to:          1 = GetStatus          2 = On          3 = Off          4 = GetCommunityString          5 = SetCommunityString</p> <p><b>--snmp_id</b>          Assigns SNMP index.          SNMP index: [1-15]</p> <p><b>--snmp_ip</b>          Sets SNMP IP.</p> <p><b>--snmp_mac</b>          Sets SNMP MAC address</p> <p><b>--community_string</b>          Sets SNMP community string</p>

#### 4.5.6. System Event Log

System Event Log	
Commands	Long Options



GetEventLog	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the event log to a file. Prints the event log onscreen if the file-saving function is not available.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p> <p><b>--raw_data (Optional)</b> Prints the raw data of each event log.</p> <p><b>--info (Optional)</b> Print the current and total capacity of event log.</p> <p><b>--mfg (Optional)</b> Prints the general information of event logs for the managed system in a style that complies with the manufacturer's assembly line requirements.</p> <p><b>--year &lt;year&gt; (Optional)</b> Filters event logs within n years.</p> <p><b>--month &lt;month&gt; (Optional)</b> Filters event logs within n months.</p> <p><b>--day &lt;day&gt; (Optional)</b> Filters event logs within n days.</p> <p><b>--format &lt;file format&gt; (Optional)</b> Saves the event log to a file in CSV format.</p> <p><b>--redfish (Optional)</b> Enables support for pure Redfish.</p>
ClearEventLog	<p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p> <p><b>--clear_bmc_eventlog (Optional)</b> Only clears the BMC event log.</p>

	<b>--clear_bios_eventlog (Optional)</b> Only clears the BIOS event log.
GetMaintenEventLog	<b>--st &lt;start time&gt; (Optional)</b> Enters the start time YYYYMMDD.  <b>--et &lt;end time&gt; (Optional)</b> Enters the end time YYYYMMDD.  <b>--file &lt;file name&gt; (Optional)</b> Saves the maintenance event log to a file. Prints the maintenance event log on screen if the file-saving function is not available.  <b>--count &lt;maintenance log count&gt; (Optional)</b> Enters the log count. If the count is equal to zero, the entire maintenance event log will display.  <b>--overwrite(Optional)</b> Overwrites the output file.
ClearMaintenEventLog	<b>--gen_log (Optional)</b> Generates a log entry indicating the successful clearing of the maintenance event log.
GetHostDump	<b>--action &lt;action&gt;</b> Sets action to: 1 = CreateDump 2 = DeleteDump 3 = DirectDump  <b>--file &lt;file name&gt; (Optional)</b> Saves the crash dump data in a file.  <b>--overwrite (Optional)</b> Overwrites the output file.

### 4.5.7. CMM Management

CMM Management (OOB Only)	
Commands	Long Options

UpdateCmm	<p><b>--file &lt;file name&gt;</b> Updates the CMM with the given image file.</p> <p><b>--individually (Optional)</b> Updates each CMM with its corresponding image file individually.</p> <p><b>--overwrite_cfg (Optional)</b> 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.</p> <p><b>--overwrite_sdr (Optional)</b> Overwrites the current CMM SDR data. (Only supported by the “CSE-947HE2C-R2K05JBOD” system.)</p> <p><b>--overwrite_ssl (Optional)</b> Overwrites the current CMM SSL configuration. (Only supported by the “CSE-947HE2C-R2K05JBOD” system.)</p> <p><b>--backup (Optional)</b> Backs up the current CMM image. (Only supported by the RoT systems.)</p> <p><b>--cmm_boot_check (Optional)</b> Checks if CMM is booted up after reset.</p>
GetCmmInfo	<p><b>--file &lt;file name&gt; (Optional)</b> Reads the CMM information from an input CMM image file.</p> <p><b>--individually (Optional)</b> Gets each CMM with its corresponding image file individually.</p> <p><b>--showall (Optional)</b> Prints the BIOS, BMC, and ARM SAA information of the managed Blade system.</p> <p><b>--file_only (Optional)</b> Works with option --file, and only reads CMM information from the input image file.</p>
GetCmmCfg	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the configuration to a file. Prints the CMM configuration on screen if the file-saving function is not available.</p> <p><b>--download (Optional)</b> Downloads the current CMM configuration file that supports profile update from CMM.</p>

	<p><b>--profile_repo (Optional)</b> Downloads existing CMM profile from CMM.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p> <p><b>--action &lt;action&gt; (Optional)</b> Sets the action for each XML table. Acceptable options: None or Change.</p>
ChangeCmmCfg	<p><b>--file &lt;file name&gt;</b> Updates the CMM with the given configuration file.</p> <p><b>--upload (Optional)</b> Uploads the CMM configuration file to CMM for updating profiles.</p> <p><b>--update &lt;update rule&gt;(Optional)</b> Updates the CMM configurations with the existing profile on CMM. Supported update rule: [Apply]</p> <p><b>--individually (Optional)</b> Updates each CMM with the corresponding configuration file individually.</p> <p><b>--precheck (Optional)</b> Checks the configurations before update.</p> <p><b>--skip_unknown (Optional)</b> Skips the unknown tables or settings in the CMM configuration file.</p> <p><b>--skip_precheck (Optional)</b> Uploads and overwrites the existing CMM profile.</p>
SetCmmPassword	<p><b>--user_id &lt;user ID&gt;</b> Enters the CMM user ID.</p> <p><b>--new_password &lt;new password&gt;</b> Sets the new CMM user password.</p> <p><b>--confirm_password &lt;confirm password&gt;</b> Confirms the new CMM user password.</p> <p><b>--pw_file &lt;password file&gt;</b> The specified file path to read the new CMM user password.</p>
LoadDefaultCmmCfg	<p><b>--clear_user_cfg</b> Clears user configuration.</p> <p><b>--preserve_user_cfg</b> Preserves user configuration.</p>

	<p><b>--load_unique_password</b> Loads CMM unique password.</p> <p><b>--load_default_password</b> Loads CMM default password</p>
GetBbpInfo	<p><b>--file &lt;file name&gt;</b> Reads the BBP information from an input BBP image file.</p> <p><b>--file_only (Optional)</b> Works with the option--file, and only reads BBP information from the input image file.</p>
UpdateBbp	<p><b>--file &lt;file name&gt;</b> Updates the BBP with the given image file.</p> <p><b>--skip_check (Optional)</b> Skips the Blade power status check to force update BBP.</p>
GetBladePowerStatus	None
SetBladePowerAction	<p><b>--action &lt;action&gt;</b> Sets power action with: 0 = down 1 = up 2 = cycle 3 = reset 5 = softshutdown 24 = accycle</p> <p><b>--blade &lt;Blade Index&gt;</b> Assigns the blade index. [A1-A14], [B1-B14] or "ALL".</p> <p><b>--node &lt;Node Index&gt; (Optional)</b> Assigns node index. [1-4]</p>
ProfileManage	<p><b>--action &lt;action&gt;</b> Supported actions: Get, Edit and Delete.</p> <p><b>--file &lt;file name&gt; (Optional)</b> Saves the profile list to a file. Prints the profile list on the screen if the file-saving function is not available.</p> <p><b>--file_id &lt;file ID&gt; (Optional)</b> Gets and edits profile information or deletes the profile on CMM with</p>

	<p>the specific file ID.</p> <p><b>--profile_name &lt;profile name&gt; (Optional)</b> Edits the profile name of the specified profile on CMM with the specific file ID.</p> <p><b>--profile_description &lt;profile description&gt; (Optional)</b> Edits the profile description of the specified profile on CMM with the specific file ID.</p> <p><b>--schedule_update_time &lt;schedule update time&gt; (Optional)</b> Edits the scheduled update time of the specified profile on CMM with the specific file ID. Format: [YYYY-MM-DD_HH:MM]</p> <p><b>--overwrite</b> Overwrites the output file.</p> <p><b>--showall</b> Gets the profile association information between the specified profile and selected Blade systems with a specific profile ID.</p>
GetBladeSwitchInfo	<p><b>--file &lt;file name&gt;</b> Reads the switch information from an input switch image file.</p> <p><b>--dev_id &lt;Device ID&gt;</b> Assigns switch index. Switch index: [A1,A2,B1,B2] or [ALL]</p> <p><b>--file_only</b> Works with --file, and only reads switch image information from the input image file.</p>
UpdateBladeSwitch	<p><b>--switch_user &lt;Switch user ID&gt;</b> Assigns switch user when updating through CMM.</p> <p><b>--switch_pw &lt;Switch user password&gt;</b> Assigns switch password when updating through CMM.</p> <p><b>--reboot</b> Forces the switch to reboot or power up after operation.</p> <p><b>--individually</b> Updates each switch module with corresponding firmware image individually.</p> <p><b>--dev_id &lt;Device ID&gt;</b> Assigns switch index when updating through CMM. Switch index: [A1,A2,B1,B2] or [ALL]</p>

RebootBladeSwitch	<p><b>--switch_user &lt;Switch user ID&gt;</b> Assigns switch user when updating through CMM.</p> <p><b>--switch_pw &lt;Switch user password&gt;</b> Assigns switch password when updating through CMM.</p> <p><b>--dev_id &lt;Device ID&gt;</b> Assigns switch index when updating through CMM. Switch index: [A1,A2,B1,B2] or [ALL]</p>
BladePSUManage	<p><b>--action &lt;action&gt;</b> Manages Blade PSU manager with these actions: GetBladePsuInfo GetBladePsuConsumption GetFanSpeed SetFanSpeed GetFanMode SetFanMode</p> <p>The following option is supported by the corresponding action. <b>--value &lt;value&gt; (Optional)</b> Assigns a value</p>
BladeSummary	None
GetCmmUserList	None
SetCmmUserList	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = Add 2 = Del 3 = Level 4 = SetPwd 5 = Test 6 = EnableType</p> <p><b>--user_id &lt;user ID&gt; (Optional)</b> The CMM user ID.</p> <p><b>--user_name (Optional)</b> The CMM user name.</p> <p><b>--user_password &lt;user password&gt; (Optional)</b> The CMM user password.</p> <p><b>--user_privilege &lt;user privilege&gt; (Optional)</b> For privilege level: Administrator: 4 Operator: 3</p>

	<p>User: 2          Callback: 1          No Access: 15          The "No Access" privilege level is not supported after AST2600 platform.</p> <p><b>--account_type &lt;account type&gt; (Optional)</b>          Supported account types for CMM management.          0 = SNMP</p> <p><b>--account_type_status &lt;account type status&gt; (Optional)</b>          Manage account type status.          0 = Disable          1 = Enable</p> <p><b>--ap &lt;authentication protocol&gt; (Optional)</b>          The authentication protocol.          0 = MD5          1 = SHA</p> <p><b>--pp &lt;private protocol&gt; (Optional)</b>          The authentication protocol.          0 = DES          1 = AES</p> <p><b>--ak &lt;authentication key&gt; (Optional)</b>          The authentication key.</p> <p><b>--pk &lt;private key&gt; (Optional)</b>          The private key.</p>
UpdateDummySwitch	<p><b>--file &lt;file name&gt; (Optional)</b>          Updates the CMM dummy switch with the given image file.</p> <p><b>--upload (Optional)</b>          Uploads the CMM dummy switch with the given image file only.</p> <p><b>--update &lt;update rule&gt; (Optional)</b>          Updates CMM dummy switch with the existing image on CMM.          Supported update rule: [Apply]</p> <p><b>--individually (Optional)</b>          Updates each CMM dummy switch with its corresponding image file individually.</p>

## 4.5.8. Storage Management



Storage Management	
Commands	Long Options
GetRaidControllerInfo	<p><b>--file &lt;file name&gt; (Optional)</b> Reads the RAID controller firmware information from an input RAID image file.</p> <p><b>--controller &lt;Controller&gt; (Optional)</b> &lt;Broadcom/Marvell&gt; Vendor of RAID controller</p> <p><b>--dev_id &lt;Device ID&gt;</b> RAID controller device ID.</p> <p><b>--file_only (Optional)</b> Works with --file, and only reads RAID controller information from the input image file.</p>
UpdateRaidController	<p><b>--file &lt;file name&gt;</b> Updates the RAID controller with the given RAID image file.</p> <p><b>--controller &lt;Controller&gt;</b> &lt;Broadcom/Marvell&gt; Vendor of RAID controller.</p> <p><b>--type &lt;Type&gt;</b> Specifies RAID type for Broadcom devices. Supported types: HBA HA-RAID</p> <p><b>--dev_id &lt;Device ID&gt;</b> Device ID of RAID controller.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
GetRaidCfg	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the configuration to a file. Prints the RAID configuration on screen if the file-saving function is not available.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p>

	<b>--controller &lt;Controller&gt; (Optional)</b> <Broadcom/Marvell> Vendor of RAID controller.
ChangeRaidCfg	<b>--file &lt;file name&gt;</b> Updates the RAID with the given configuration file.  <b>--individually (Optional)</b> Updates the RAID with the given configuration file.  <b>--controller &lt;Controller&gt; (Optional)</b> <Broadcom/Marvell> Vendor of RAID controller.
GetSataInfo (OOB only)	None
GetNvmeInfo (OOB only)	<b>--dev_id &lt;Device ID&gt; (Optional)</b> NVMe device controller ID. Prints all NVMe information on the screen if the file-saving function is not available.
GetPMemInfo	<b>--file &lt;file name&gt; (Optional)</b> Reads the PMem information from an input PMem image file.  <b>--file_only (Optional)</b> Works with --file, and only reads PMem information from the input image file.
UpdatePMem	<b>--file &lt;file name&gt; (Optional)</b> Updates the PMem with the given PMem firmware file.  <b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.  <b>--restore_default_fw (Optional)</b> Updates the PMem with BIOS built-in PMem firmware.

	<p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--post_complete (Optional)</b> UWaits for the managed system's POST to complete after reboot.</p>
GetVROCCfg	<p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
ChangeVROCCfg	<p><b>--file &lt;file name&gt;</b> Updates the VROC with the given configuration file.</p> <p><b>--individually (Optional)</b> Updates each VROC key with the corresponding configuration file individually.</p>
ControlNVMe	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = Locate 2 = StopLocate 3 = Insert 4 = Remove 5 = Rescan</p> <p><b>--dev_id</b> The NVMe controller ID can be found using the GetNvmeInfo command.</p>

	<p><b>--group_id</b> The NVMe device group ID can be found using the GetNvmeInfo command.</p> <p><b>--slot</b> The NVMe slot number can be found using the GetNvmeInfo command.</p>
GetSmartData	<p><b>--device_name &lt;HDD Name&gt; (Optional)</b> Gets the specified device's smart data</p>
GetSasExpanderInfo	<p><b>-I Redfish_HI (Optional)</b> Uses Redfish Host Interface to query the firmware information. (Only in-band usage is supported.)</p> <p><b>--file &lt;file name&gt; (Optional)</b> Reads the SAS Expander information from an input image file.</p> <p><b>--file_only (Optional)</b> Works with the --file option, and only reads SAS Expander information from the input image file.</p>
UpdateSasExpander	<p><b>--file &lt;file name&gt;</b> Updates SAS Expander with the given image file.</p> <p><b>--index &lt;index&gt;</b> Set the SAS Expander index that needs to be updated.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>-I Redfish_HI (Optional)</b> Uses Redfish Host Interface to query the firmware information. (Only in-band usage is supported.)</p>

### 4.5.9. Power Management

#### Power Management

Commands	Long Options
GetPsuInfo	None
UpdatePsu	<p><b>--file &lt;file name&gt;</b> PSU firmware file.</p> <p><b>--address</b> PSU module address in HEX format (Gets PSU module slave address from the GetPSUInfo command.)</p>
GetPowerStatus	None
SetPowerAction	<p><b>--action &lt;action&gt;</b> Sets power action with 0 = up 1 = down 2 = cycle 3 = reset 4 = softshutdown 5 = reboot  6 = accycle</p> <p><b>--interval &lt;time interval&gt; (Optional)</b> Sets the power cycle interval in seconds.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
DcmiManage	<p><b>--type &lt;type&gt;</b> Manages system with type: STD_DCMI NM20</p> <p><b>--action &lt;action&gt;</b> Manages system with action for --type STD_DCMI: Find GetCap GetPowerStatus GetMCID SetMCID</p> <p>Manages system with action for --type NM20: GetCap GetPowerReading GetPowerLimit SetPowerLimit EnablePowerLimit</p>

	<p>DisablePowerLimit</p> <p>The following options are supported by the corresponding action.</p> <p><b>--start_ip &lt;Start IP&gt; (Optional)</b> Assigns start IP.</p> <p><b>--end_ip &lt;End IP&gt; (Optional)</b> Assigns end IP.</p> <p><b>--netmask &lt;Netmask&gt; (Optional)</b> Assigns netmask.</p> <p><b>--value &lt;Value&gt; (Optional)</b> Assigns value.</p> <p><b>--mode &lt;Mode&gt; (Optional)</b> Assigns mode.</p> <p><b>--limit &lt;Limit&gt; (Optional)</b> Assigns limit.</p> <p><b>--period &lt;Period&gt; (Optional)</b> Assigns period.</p> <p><b>--exception_action &lt;Exception action&gt; (Optional)</b> Assigns mode.</p> <p><b>--time &lt;Time&gt; (Optional)</b> Assigns time.</p>
PowerPolicy	<p><b>--type &lt;type&gt;</b> Manages system with type: NM20 BMC10</p> <p><b>--action &lt;action&gt;</b> Manages system with action for --type NM20: EnableGlobal DisableGlobal EnableDomain DisableDomain EnablePolicy DisablePolicy AddPowerPolicy GetPolicy DelPolicy ScanPolicy AddPolicy GetAlertThreshold SetAlertThreshold</p>

---

GetPeriod  
AddPeriod  
UpdatePeriod  
DeletePeriod  
ClearPeriod

Manages system with action for --type BMC10:

EnableGlobal  
DisableGlobal  
EnableDomain  
DisableDomain  
EnablePolicy  
DisablePolicy  
AddPowerPolicy  
GetPolicy  
DelPolicy  
ScanPolicy  
AddPolicy  
GetLimitPolicyId

The following options are supported by the corresponding action.

**--count <Count> (Optional)**

Assigns count.

**--limit <Limit> (Optional)**

Assigns limit.

**--mode <Mode> (Optional)**

Assigns mode.

**--period <Period> (Optional)**

Assigns period.

**--exception\_action <Exception action> (Optional)**

Assigns mode.

**--time <Time> (Optional)**

Assigns time.

**--policy\_id <Policy ID> (Optional)**

Assigns policy id.

**--domain\_id <Domain ID> (Optional)**

Assigns domain ID.

**--trigger\_type <Trigger TYPE> (Optional)**

Assigns trigger type.

**--trigger\_limit <Trigger Limit> (Optional)**

Assigns trigger limit.

	<p><b>--storage &lt;Storage&gt; (Optional)</b> Specify storage option. 0: Persistent storage (default) 1: Volatile memory</p> <p><b>--overwrite (Optional)</b> Overwrites the policy.</p> <p><b>--value &lt;Value&gt; (Optional)</b> Assigns value.</p> <p><b>--st &lt;Start time&gt; (Optional)</b> Assigns start time.</p> <p><b>--et &lt;End time&gt; (Optional)</b> Assigns end time.</p> <p><b>--days &lt;Day&gt; (Optional)</b> Assigns days.</p>
GetAcpiPowerStatus	None
GetAiomStandbyPower	None
SetAiomStandbyPower	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = On 2 = Off</p>

### 4.5.10. Applications

Applications	
Commands	Long Options
RawCommand	<p><b>--raw &lt;raw command&gt;</b> Inputs hex-value commands</p> <p><b>--ipmb &lt;raw command&gt;</b> Inputs hex-value commands.</p>
GetUsbAccessMode (Inband Only)	None
SetUsbAccessMode (Inband Only)	<p><b>--panel &lt;front/rear&gt;</b> The panel to be set.</p>



	<p><b>--enable</b> Dynamically enables the USB ports in the assigned panel.</p> <p><b>--disable &lt;front/rear&gt;</b> Dynamically disables the USB ports in the assigned panel.</p>
KmsManage	<p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--server_ip &lt;server IP address&gt; (Optional)</b> Enters a KMS server IP address.</p> <p><b>--second_server_ip &lt;second server IP address&gt; (Optional)</b> Enters a second KMS server IP address.</p> <p><b>--port &lt;port&gt; (Optional)</b> Command optional port(s). The format of &lt;port&gt; is "TCP:5696" or "5696". TCP is served as the KMS server port.</p> <p><b>--time_out &lt;time out&gt; (Optional)</b> Enters a KMS server connecting time-out.</p> <p><b>--time_zone &lt;time zone&gt; (Optional)</b> Enters a correct time zone GMT+.</p> <p><b>--client_username &lt;client username&gt; (Optional)</b> Enters a client identity: UserName.</p> <p><b>--client_password &lt;client password&gt; (Optional)</b> Enters a client identity: Password.</p> <p><b>--ca_cert &lt;CA certificate file name&gt; (Optional)</b> Uploads a CA certificate from the file.</p> <p><b>--client_cert &lt;client certificate file name&gt; (Optional)</b> Uploads a client certificate from the file.</p> <p><b>--pvt_key &lt;private key file name&gt; (Optional)</b> Uploads a client private key from the file.</p> <p><b>--pvt_key_pw &lt;private key password&gt; (Optional)</b> Enters client private key password.</p>

	<p><b>--file &lt;file name&gt; (Optional)</b> When the --action GetInfo option is specified, it saves the OEM configuration to a file; otherwise, it updates the OEM settings with the given configuration file.</p> <p><b>--overwrite (Optional)</b> Overwrites the output file.</p> <p><b>--individually (Optional) (Optional)</b> Updates the OEM settings of each BIOS with its corresponding configuration file individually.</p> <p><b>--action &lt;action&gt; (Optional)</b> WSets a KMS manage action to: 1 = GetInfo 2 = Probe 3 = DeleteCA 4 = DeleteCert 5 = DeletePvtKey 6 = DeleteAll</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
RedfishApi	<p><b>-v</b> Verbose output: prints the response header.</p> <p><b>--file &lt;file name&gt;</b> Outputs the result to a file.</p> <p><b>--overwrite</b> Overwrites the output file.</p> <p><b>--individually</b> Reads the request body from the file individually. (Only support for Multiple systems OOB usage)</p> <p><b>--request &lt;HTTP method&gt;</b> HTTP method (GET, POST, or PATCH)</p> <p><b>--data &lt;Request body&gt;</b> Request body.</p>

	<b>--retry &lt;Number&gt;</b> Number of retry times. The default value is 3.
RemoteExec	<b>-I Remote_INB</b> Manages the remote systems and executes commands with in-band usage.  <b>--remote_cmd &lt;Remote command&gt;</b> Enters the commands to be executed on remote Linux systems.  <b>--file &lt;file name&gt;</b> Transfers the file(s) to a remote system.
RemoteConsole	None.
RemoteScreenshot	<b>--file</b> Saves the screen shot to a file. <b>--overwrite (Optional)</b> Overwrites the output file.
RemoteKeyboard	<b>--file (Optional)</b> Reads keyboard operations from specified file. <b>--showall (Optional)</b> Shows all supported keys and some samples.
SOL	<b>--action &lt;action&gt;</b> Sets action to: 1 = Activate 2 = Deactivate 3 = GetInfo 4 = Set  <b>--bitrate &lt;bitrate&gt; (Optional)</b> SOL transmission bit rate. Available SOL bit rate: [9.6 19.2 38.4 57.6 115.2] (kbps) (Only supported with the Set action.)  <b>--retryCount &lt;retry count&gt; (Optional)</b> SOL retry counts. (Only supported with the Set action.)  <b>--retryInterval &lt;retry interval&gt; (Optional)</b> The interval for BMC to retry sending SOL packets to the remote console. The retry interval is set in milliseconds, and the value should be

	<p>ten or a multiple of ten. (Only supported with the 'Set' action.)</p>
FindBmcDevices	<p><b>--file &lt;file name&gt; (Optional)</b> The file to write, required with --getMACs used.</p> <p><b>--start_ip &lt;Start IP&gt; (Optional)</b> Start address of the network to search.</p> <p><b>--end_ip &lt;End IP&gt; (Optional)</b> End address of the network to search.</p> <p><b>--netmask &lt;Netmask&gt; (Optional)</b> Subnet mask of the network to search.</p> <p><b>--getMACs &lt;Get the MAC addresses of available BMC devices&gt; (Optional)</b> Retrieves the MAC addresses of the found BMC devices and writes them to a file.</p> <p><b>--find_user &lt;Username for find device&gt; (Optional)</b> Specifies the username for the found BMC devices. This option should be used in conjunction with the --getMACs option.</p> <p><b>--find_password &lt;Password for find device&gt; (Optional)</b> Specifies the password for the found BMC devices. This option should be used in conjunction with "getMACs."</p>
FoundBmcDevices	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = List 2 = Clear 3 = Copy 4 = CopyAll 5 = SaveAs 6 = Refresh</p> <p><b>--file &lt;file name&gt; (Optional)</b> Specifies the name of the file to write. This option is required when using the "saveAs" command.</p> <p><b>--index &lt;index&gt; (Optional)</b> Specifies the indices of the host to be copied. This option is required when using the "Copy" action.</p>

Shell (OOB only)	None
Prompt (Inband Only)	<p><b>--item &lt;item name&gt;</b> Gets/Sets the prompt value for the given prompt item. 1 = all 2 = time 3 = fwver 4 = username 5 = ip 6 = mb 7 = power 8 = acpi</p> <p><b>--action &lt;action&gt;</b> Sets action to: 1 = Get 2 = Set</p> <p><b>--enable (Optional)</b> Enables the prompt value for the specified prompt item.</p> <p><b>--disable (Optional)</b> Disables the prompt value for the specified prompt item.</p>

### 4.5.11. GPU Management

GPU Management	
Commands	Long Options
GetGPUInfo	<p><b>--showall</b> Prints the FRU information on the GPU baseboard of the managed system. (Only supports on X11/H11 with HGX2 system and Intel Gaudi 2/3 system.)</p> <p><b>--showoam (Optional)</b> For Intel PVC and Intel Gaudi2 system shows individual OAM.</p> <p><b>--file &lt;file name&gt;(Optional)</b> Reads the GPU information from an input GPU image file.</p> <p><b>--file_only (Optional)</b> Works with --file, and only reads GPU information from the input image file.</p>
UpdateGPU	<p><b>--file &lt;file name&gt;</b> Updates the GPU firmware file that matches the FW item types.</p>

	<p><b>--item &lt;item name&gt;</b> FW item types of GPU firmware:</p> <p>1 = CEC 2 = FPGA 3 = HGX_H100 4 = PVC_IFWI 5 = PVC_PSCBIN 6 = PVC_UBB_CPLD 7 = PVC_RETIMER 8 = PVC_AMC 9 = GAUDI_SPI 10 = GAUDI_OAM_CPLD 11 = GAUDI_RETIMER 12 = GAUDI_UBB_CPLD 13 = H100_FPGA 14 = H100_HMC 15 = H100_HMC_EROT 16 = H100_FPGA_EROT 17 = H100_PCIESWITCH 18 = H100_PCIESWITCH_EROT 19 = H100_GPU 20 = H100_GPU_EROT 21 = H100_NVSWITCH 22 = H100_NVSWITCH_EROT 23 = H100_RETIMER 24 = MGX_GPU 25 = MI300X 26 = ONBOARD_RETIMER</p> <p><b>--dev_id &lt;Device ID&gt; (Optional)</b> Retrieved Device ID with the GetGPUInfo command. For SPI-FW, use the device Address. For H100 Retimer, H100 GPU, H100 GPU ERoT, H100 NVSwitch and H100 NVSwitch ERoT, use the device id.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
DiagGpuStatus	<p><b>--dev_id &lt;Device ID List&gt; (Optional)</b> The device ID list of GPU on the managed system.</p>
GetGpuLog	<p><b>--file &lt;file name&gt;</b> Saves the GPU log to a file.</p> <p><b>--item &lt;item name&gt;</b> Item type of GPU: 1 = HGX_H100</p>

	<p>2 = MI300X</p> <p><b>--type &lt;type&gt;</b>  1 = DebugToken  (This option is only used for downloading Debug Token certificate log file.)</p> <p><b>--overwrite</b>  Overwrites the output file.</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 4.5.12. CPLD Management

CPLD Management	
Commands	Long Options
GetCpldInfo	<p><b>--individually (Optional)</b>  Gets each CPLD with its corresponding image file individually.</p> <p><b>--file &lt;file name&gt; (Optional)</b>  Reads the CPLD information from an input CPLD image file.</p> <p><b>--file_only (Optional)</b>  Works with the --file option, and only reads CPLD information from the input image file.</p> <p><b>--extract_measurement (Optional)</b>  Works with the --file option, extract CPLD image file measurement if supported.</p>
UpdateCpld	<p><b>--file &lt;file name&gt;</b>  Updates the CPLD with the given CPLD image file.</p> <p><b>--reboot</b>  Forces the managed system to reboot or power up after operation.</p> <p><b>--individually (Optional)</b>  Updates each CPLD with corresponding configuration file individually.</p> <p><b>--post_complete (Optional)</b>  Waits for the managed system's POST to complete after rebooting.</p> <p><b>--index &lt;number&gt; (Optional)</b></p>

	Updates the CPLD with the given index. The default value is empty, and the first CPLD will be updated.
GetSwitchboardCpldInfo	None
UpdateSwitchboardCpld	<p><b>--file &lt;file name&gt;</b> Updates the Main or Side Switchboard CPLD with the given image file.</p> <p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--type</b> Sets action to: 1 = Main 2 = Left 3 = Right</p> <p><b>--individually (Optional)</b> Updates each CPLD Switch Board with its corresponding configuration file individually.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after rebooting.</p> <p><b>--index &lt;number&gt; (Optional)</b> Sets the CPLD index. The default value is 1, and the index count starts from 1.</p>
GetBackplaneCpldInfo	None
UpdateBackplaneCpld	<p><b>--manual_ejected</b> Confirmed that all drives on backplane have been ejected manually.</p> <p><b>--file &lt;file name&gt;</b> Updates the Backplane CPLD with the given FW image file.</p> <p><b>--index &lt;number&gt;</b> Updates the specific Backplane CPLD with the given index.</p> <p><b>--dev_id &lt;number&gt; (Optional)</b> Set the CPLD index, default value is 1.</p>



	<p><b>--update_list &lt;item list&gt; (Optional)</b>  Updates multiple backplane CPLDs with one command, using a comma (",") to distinguish between items.  Item list example: 1:CPLD.jed,2:CPLD.jed...</p> <p><b>--individually (Optional)</b>  Updates each backplane CPLD with its corresponding image file individually.</p>
GetFanboardCpldInfo	None
UpdateFanboardCpld	<p><b>--file &lt;file name&gt;</b>  Updates the Fanboard CPLD with the given Fanboard CPLD image file.</p> <p><b>--type</b>  Sets action to:  1 = Front  2 = Rear  or the corresponding Fanboard ID number.</p> <p><b>--index &lt;number&gt; (Optional)</b>  Set the CPLD index, default value is 1. The index count starts from 1.</p> <p><b>--individually (Optional)</b>  Updates each Fanboard CPLD with corresponding configuration file individually.</p>
GetAipCpldInfo (OOB only)	None
UpdateAipCpld (OOB only)	<p><b>--file &lt;file name&gt;</b>  Updates the CPLD of AIP with the given FW image file.</p> <p><b>--individually (Optional)</b>  Updates each AIP CPLD with its corresponding image file individually.</p>
GetAomboardCpldInfo	None
UpdateAomboardCpld	<p><b>--file &lt;file name&gt;</b>  Updates the AOM board CPLD with the given CPLD image file.</p>

	<p><b>--individually (Optional)</b> Updates each AOM board CPLD with its corresponding image file individually.</p> <p><b>--dev_id &lt;Device ID&gt; (Optional)</b> Updates the AOM board CPLD with the given AOM device ID. The default value is empty, and the CPLD for the first AOM board will be updated.</p> <p><b>--index &lt;number&gt; (Optional)</b> Updates the CPLD with the given index. The default value is empty, and the first CPLD on the AOM board will be updated.</p>
GetMiscCpldInfo	None
UpdateMiscCpld	<p><b>--file &lt;file name&gt;</b> Updates the motherboard Miscellaneous CPLD with the given CPLD image file.</p> <p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--individually (Optional)</b> Updates each motherboard Miscellaneous CPLD with its corresponding image file individually.</p>
GetMidplaneSbbCpldInfo	<p><b>-I Redfish_HI (Optional)</b> Uses Redfish Host Interface to query the firmware information. (Only in-band usage is supported.)</p>
UpdateMidplaneSbbCpld	<p><b>--file &lt;file name&gt;</b> Updates the Midplane SBB CPLD with the given CPLD image file.</p> <p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--index &lt;number&gt;</b> Sets the CPLD index.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after</p>

	rebooting.  <b>--individually (Optional)</b> Updates each Midplane SBB CPLD with its corresponding image file individually.
GetNICCpldInfo	None
UpdateNICCpld	<b>--file &lt;file name&gt;</b> Updates the NIC CPLD with the given CPLD image file.  <b>--individually (Optional)</b> Updates each CPLD on NIC with its corresponding image file individually.  <b>--dev_id &lt;Device ID&gt; (Optional)</b> Updates the CPLD on NIC with the given NIC ID and CPLD ID. The CPLD for the first NIC will be updated by default. e.g., NIC 1 and CPLD 1: --dev_id 1_1
GetTransitionboardCpldInfo	None
UpdateTransitionboardCpld	<b>--file &lt;file name&gt;</b> Updates the Transitionboard CPLD with the given CPLD image file.  <b>--individually (Optional)</b> Updates each Transitionboard CPLD with its corresponding image file individually.

### 4.5.13. NIC Management

NIC Management	
Commands	Long Options
GetAocNICInfo	<b>--file &lt;file name&gt;</b> Reads the AOC NIC firmware information from an input AOC_NIC image file.  <b>--dev_id &lt;DEVICE_ID&gt;(Optional)</b> AOC NIC device ID list.

	<b>--file_only (Optional)</b> Works with the --file option, and only reads AOC-NIC information from the input image file.
UpdateAocNIC	<b>--file &lt;file name&gt;</b> Updates AOC NIC with the given add-on NIC file.  <b>--reboot</b> Forces the managed system to reboot or power up after operation.  <b>--dev_id &lt;DEVICE ID&gt;</b> Device ID of AOC NIC.  <b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.

#### 4.5.14. VM Management

VM Management	
Commands	Long Options
MountIsoImage	<b>--image_url &lt;URL&gt;</b> 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>&lt;shared point>&lt;file path>' HTTP URL: 'http://<host name or ip>/<shared point>/<file path>'  <b>--id &lt;ID&gt; (Optional)</b> The specified ID to access the shared file.  <b>--pw &lt;Password&gt; (Optional)</b> The specified password to access the shared file.  <b>--pw_file &lt;Password File&gt; (Optional)</b> The specified file path to read the password.  <b>--redfish (Optional)</b> Enables support for pure Redfish.
UnmountIsoImage	<b>--redfish (Optional)</b> Enables support for pure Redfish.
MountFloppyImage	<b>--file &lt;file name&gt;</b> Mounts the specified binary floppy file to the managed system.
UnmountFloppyImage	None

GetVmInfo	<p><b>--dev_id &lt;Device ID&gt; (Optional)</b>          Uses the specified device ID to get virtual media information.          The supported device ID: [1-3]</p>
VmManage	<p><b>--action &lt;action&gt;</b>          Sets action to:          1 = Enable          2 = Disable          3 = Mount          4 = Unmount</p> <p><b>--port &lt;port&gt; (Optional)</b>          Command optional port(s)          The format is "VM:623" or "623."          Command optional port(s) list:</p> <ol style="list-style-type: none"> <li>1. VM (for virtual media port)</li> </ol> <p><b>--image_url &lt;URL&gt;</b>          The URLs to access the shared image file.          SAMBA URL: 'smb://&lt;host name or ip&gt;/&lt;shared point&gt;/&lt;file path&gt;'          SAMBA UNC: '\\&lt;host name or ip&gt;&amp;lt;shared point&gt;&amp;lt;file path&gt;'          HTTP URL: 'http://&lt;host name or ip&gt;/&lt;shared point&gt;/&lt;file path&gt;'</p> <p><b>--id &lt;ID&gt; (Optional)</b>          The specified ID to access the shared file.</p> <p><b>--pw &lt;Password&gt; (Optional)</b>          The specified password to access the shared file.</p> <p><b>--pw_file &lt;Password File&gt; (Optional)</b>          The specified file path to read the password.</p> <p><b>--dev_id &lt;Device ID&gt; (Optional)</b>          The specified device ID to manage virtual media device.          The supported device ID: [1-3]          Support [All] for action Unmount to unmount all devices.</p> <p><b>--verify_cert (Optional)</b>          Verifies the SSL certificate. (Only supported for HTTPS protocol.)</p> <p><b>--accept_self_signed (Optional)</b>          Accepts the self-signed certificate. (Only supported for HTTPS protocol.)</p>
VMShell	<p><b>This command is only available in SAA shell mode.</b></p> <p><b>--action &lt;action&gt;</b></p>

	<p>Sets action to:</p> <ul style="list-style-type: none"> <li>1 = devlist</li> <li>2 = dev1drv</li> <li>3 = dev1stop</li> <li>4 = dev2iso</li> <li>5 = dev2stop</li> <li>6 = status</li> <li>7 = log</li> </ul> <p><b>--file &lt;file name&gt; (Optional)</b> Mounts the ISO image file for virtual media device 2. Use it with the dev2iso action.</p> <p><b>--dev_id &lt;Device ID&gt; (Optional)</b> Uses the specified device ID to get virtual media information. The supported device ID is [1-3]. Use it with the Status action.</p> <p><b>--index &lt;index&gt; (Optional)</b> Mounts the drive with specified index for virtual media device 1. Use it with the dev1drv actions.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 4.5.15. NM Management

NM Management	
Commands	Long Options
NmMeManage	<p><b>--type &lt;type&gt;</b> Manages Intel Node Manager with type: NM20</p> <p><b>--action &lt;action&gt;</b> Manages Intel Node Manager with action: GetDeviceID Reset ResetToDefault EnterToUpdateMode PowerOff SelfTest Mode ListImagesInfo GetPower GetTemp</p>
GeneralNmManage	<p><b>--type &lt;type&gt;</b> Manages Intel Node Manager with type: NM20 BMC10</p>

---

**--action <action>**

Manages Intel Node Manager with action for --type NM20:

GetNMSDR  
GetSelTime  
GetStatistics  
ResetStatistics  
GetCapabilities  
GetVersion  
GetAlert  
SetAlert  
GetTotalPower  
SetTotalPower  
DelTotalPower  
SetPowerDrawRange  
GetSensor  
GetSummary

Manages Intel Node Manager with action for --type BMC10:

GetSelTime  
GetStatistics  
ResetStatistics  
GetCapabilities  
GetVersion  
GetTotalPower  
SetTotalPower  
DelTotalPower  
SetPowerDrawRange  
GetSummary

The following options are supported by the corresponding action.

**--mode <type> (Optional)**

Assigns mode.

**--policy\_id <Policy ID> (Optional)**

Assigns policy ID.

**--domain\_id <Domain ID> (Optional)**

Assigns domain ID.

**--trigger\_type <Trigger Type> (Optional)**

Assigns trigger type.

**--value <Assignment value> (Optional)**

Assigns value.

**--range <Range> (Optional)**

Assigns value range.

**--per\_component\_control <Per-component Control> (Optional)**

	<p>Allows for setting the power budget for a chosen domain component.</p> <p><b>--component_id &lt;Component ID&gt; (Optional)</b> Assigns a component ID.</p>
NmCpuManage	<p><b>--type &lt;type&gt;</b> Manages CPU with type: NM20 NM40</p> <p><b>--action &lt;action&gt;</b> Manages CPU with action: Manages system with action for --type NM20: GetPState GetTState GetPTState GetCPUCores GetCPUMemTemp GetHostCPUData SetMaxAllowedPState SetMaxAllowedTState SetMaxAllowedCPUCores Manages system with action for --type NM40: GetTurboSyncRatio SetTurboSyncRatio</p> <p>The following options are supported by the corresponding action.</p> <p><b>--value &lt;Assignment value&gt; (Optional)</b> Assigns value.</p> <p><b>--socket &lt;Socket number&gt; (Optional)</b> Assigns socket number.</p> <p><b>--limit &lt;limit&gt; (Optional)</b> Assigns limit.</p> <p><b>--core &lt;Core number&gt; (Optional)</b> Assigns core number.</p>
NmCupsManage	<p><b>--type &lt;type&gt;</b> Manages Compute Usage Per Second(CUPS) with type: NM30</p> <p><b>--action &lt;action&gt;</b> Manages Compute Usage Per Second(CUPS) with action: GetCUPSCapability GetCUPSData GetCUPSConfig GetCUPSPolicy GetCUPSCore</p>



	<p>GetCUPSIO GetCUPSMem SetCUPSPolicy EnableCUPSPolicy DisableCUPSPolicy</p> <p>The following options are supported by the corresponding action.</p> <p><b>--value &lt;Assignment value&gt; (Optional)</b> Assigns value.</p> <p><b>--domain_id &lt;Domain ID&gt; (Optional)</b> Assigns domain ID.</p> <p><b>--storage &lt;Storage&gt; (Optional)</b> Assigns sotrage.</p> <p><b>--alert &lt;Alert&gt; (Optional)</b> Assigns alert status.</p> <p><b>--threshold &lt;Threshold&gt; (Optional)</b> Assigns CUPS threshold(0~100).</p> <p><b>--avg_windows &lt;averaging window&gt; (Optional)</b> Assigns averaging window in seconds(0~65535).</p>
BmcNmManage	<p><b>--type &lt;type&gt;</b> Manages Intel Node Manager with a type: BMC10</p> <p><b>--action &lt;action&gt;</b> Manages Intel BMC Node Manager with an action: GetDeviceID GetPower GetTemp</p>

#### 4.5.16. Multi-Node Management

Multi-Node Management	
Commands	Long Options
GetTplInfo	<p><b>--file &lt;file name&gt; (Optional)</b> Saves the configuration to a file. Prints the TwinPro configuration on the screen if the file-saving function is not available.</p>

	<b>--overwrite (Optional)</b> Overwrites the output file.
ChangeTpInfo	<b>--file &lt;file name&gt;</b> Updates the TwinPro configuration with the given configuration file.  <b>--individually (Optional)</b> Updates each set of TwinPro configurations with the corresponding configuration file individually.
GetMultinodeEcInfo	<b>--file &lt;file name&gt; (Optional)</b> Reads the multi-node EC information from an input multi-node EC image file.  <b>--file_only (Optional)</b> Works with the --file option, and only reads multi-node EC information from the input image file.
UpdateMultinodeEc	<b>--file &lt;file name&gt;</b> Updates the multi-node EC with the given multi-node EC image file.

## 4.5.17. FPGA Management

FPGA Management	
Commands	Long Options
GetMotherboardFpgaInfo	<b>--file &lt;file name&gt; (Optional)</b> Reads the motherboard FPGA information from an input FPGA image file.  <b>--file_only (Optional)</b> Works with the --file option, and only reads motherboard FPGA information from the input image file.
UpdateMotherboardFpga	<b>--file &lt;file name&gt;</b> Updates the motherboard FPGA with the given FPGA image file.  <b>--reboot</b> Forces the managed system to reboot or power up after operation.  <b>--individually (Optional)</b>

	Updates each motherboard FPGA with corresponding image file individually.
--	---------------------------------------------------------------------------

#### 4.5.18. PCIeSwitch Management

PCIeSwitch Management	
Commands	Long Options
GetPCIeSwitchInfo	<p><b>--file &lt;file name&gt; (Optional)</b> Reads the PCIe Switch information from an input PCIe Switch image file.</p> <p><b>--showall (Optional)</b> Shows additional information about the PCIe Switch device.</p> <p><b>--file_only (Optional)</b> Works with the --file option, and only reads PCIe Switch information from the input image file.</p>
UpdatePCIeSwitch	<p><b>--file &lt;file name&gt; (Optional)</b> PCIe switch firmware file.</p> <p><b>--dev_id &lt;Device ID&gt;</b> PCIe switch device ID. Can be retrieved with GetPCIeSwitchInfo command.</p> <p><b>--reboot (Optional)</b> Forces the managed system to power cycle after operation.</p>

#### 4.5.19. Security Management

Security Management	
Commands	Long Options
BiosRotManage	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = GetInfo 2 = UpdateGolden 3 = Recover 4 = DownloadEvidence</p> <p><b>--file &lt;file name&gt; (Optional)</b> Works with --action DownloadEvidence. Saves the BIOS evidence to a file.</p>

	<p><b>--overwrite (Optional)</b> Works with --action DownloadEvidence. Overwrites the output file.</p> <p><b>--reboot (Optional)</b> Works with --action UpdateGolden and Recover. Forces the managed system to reboot or power up after operation.</p> <p><b>--redfish (Optional)</b> Enables pure Redfish support.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
BmcRotManage	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = GetInfo 2 = UpdateGolden 3 = Recover 4 = DownloadEvidence</p> <p><b>--file &lt;file name&gt; (Optional)</b> Works with --action DownloadEvidence. Saves the BMC evidence to a file.</p> <p><b>--overwrite (Optional)</b> Works with --action DownloadEvidence. Overwrites the output file.</p> <p><b>--redfish (Optional)</b> Enables support for pure Redfish.</p>
CpldRotManage	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = GetInfo 2 = UpdateGolden</p>
SecureBootManage	<p><b>--action &lt;action&gt;</b> Sets action to: 1 = Status 2 = Enable 3 = Disable 4 = Showdatabases 5 = UploadCertificate 6 = ResetAllKeysToDefault 7 = DeleteAllKeys 8 = DeletePK</p> <p><b>--file_type &lt;file type&gt; (Optional)</b></p>

	<p>Selects the type of secure boot key. The format of &lt;file type&gt; includes "PK," "KEK," "db," "dbr," "dbt" or "dbx" (case sensitive). Note that "dbx" can be only used with the "ShowDatabases" action</p> <p><b>--file (Optional)</b> Uploads secure boot key in the format of PEM.</p> <p><b>--individually (Optional)</b> Updates each system secure boot keys individually with the corresponding secure boot key.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
GetLockdownMode	None
SetLockdownMode	<p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--lock &lt;yes/no&gt;</b> Locks/Unlocks the managed system.</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
Attestation	<p><b>--action &lt;action&gt;</b> Sets action to: Dump List Download Delete GetInfo Comapre</p> <p><b>--file &lt;file name&gt; (Optional)</b> File name for the measurement file on managed system or local storage.</p> <p><b>--ref &lt;file name&gt; (Optional)</b> Reference measurement file for comparison. (Only supported with the Compare action)</p> <p><b>--overwrite (Optional)</b> Overwrites the downloaded or extracted file.</p>

	<p><b>--showall (Optional)</b> Prints all information from the measurement file. (Only supported with the GetInfo action)</p> <p><b>--item &lt;item name&gt; (Optional)</b> Prints the specified item for the measurement file. (Only supported with the GetInfo action)</p> <p><b>--file_only (Optional)</b> Gets information from the local measurement file. (Required option for the GetInfo action)</p> <p><b>--root_cert &lt;file name&gt; (Optional)</b> Inputs the public certificate of Root CA to verify the certificate chain in measurement file. (Only supported with the GetInfo action)</p> <p><b>--extract_certs &lt;file name&gt; (Optional)</b> Extracts endpoint certificate chain from the local measurement file. (Only supported with the GetInfo action)</p> <p><b>--nonce &lt;nonce&gt; (Optional)</b> Specify nonce for action Dump.</p> <p><b>--type (Optional)</b> Specifies the dump type for the Dump action. Supported types: MB</p>
SecureEraseRaidHdd	<p><b>--dev_id &lt;Device ID&gt;</b> A RAID controller ID for secure erase.</p> <p><b>--enc_id &lt;Enclosure ID&gt;</b> Enclosure ID list or "ALL" in the RAID controller for secure erase.</p> <p><b>--dsk_id &lt;Disk ID&gt;</b> Disk ID list or "ALL" in the RAID controller for secure erase.</p> <p><b>--tsk_id &lt;Task ID&gt; (Optional)</b> Accesses the progress of a secure erase.</p> <p><b>--precheck (Optional)</b> Display detail information for the list of the RAID controller.</p> <p><b>--abort (Optional)</b> Stop the list of RAID controller secure erase action.</p> <p><b>--sync (Optional)</b></p>

	Shows the current progress of the secure-erase operation of the RAID controller.
SecureEraseDisk	<p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--cur_pw_file &lt;Current Password File&gt; (Optional)</b> The specified file path to read the current password.</p> <p><b>--file &lt;file name&gt;</b> HDD serial number mapping file.</p> <p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--precheck (Optional)</b> Only displays HDD status.</p> <p><b>--action &lt;action&gt; (Optional)</b> Sets secure erase action to: 1 = SetPassword 2 = SecurityErase 3 = SecurityErasePWD 4 = SecurityErasePSID 5 = ChangePassword 6 = ClearPassword</p> <p><b>--post_complete (Optional)</b> Waits for the managed system's POST to complete after reboot.</p>
TpmProvision (OOB only)	<p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--image_url &lt;URL&gt;</b> The URLs to access the shared image file. SAMBA URL: 'smb://&lt;host name or ip&gt;/&lt;shared point&gt;/&lt;file path&gt;' SAMBA UNC: '\\&lt;host name or ip&gt;&amp;lt;shared point&gt;&amp;lt;file path&gt;' HTTP URL: 'http://&lt;host name or ip&gt;/&lt;shared point&gt;/&lt;file path&gt;'</p> <p><b>--lock &lt;yes&gt;</b> Locks the TPM module.</p> <p><b>--id &lt;ID&gt; (Optional)</b> Allows the specified ID to access the shared file.</p> <p><b>--pw &lt;Password&gt; (Optional)</b> The specified password to access the shared file.</p>

	<p><b>--pw_file &lt;Password File&gt; (Optional)</b> Allows the specified file path to read password.</p> <p><b>--cleartpm (Optional)</b> Clears the ownership of the TPM module and restores the relevant TPM BIOS settings.</p>
GetTpmInfo	<p><b>--current_password &lt;current password&gt; (Optional)</b> Checks the current BIOS Administrator password.</p> <p><b>--showall (Optional)</b> Prints the NV data and the capability flags (if applicable) of the trusted platform module. (Only supported for Intel platforms)</p> <p><b>--cur_pw_file &lt;Current password file&gt; (Optional)</b> The specified file path to read the current password.</p>
TpmManage	<p><b>--reboot (Optional)</b> Forces the managed system to reboot or power up after operation.</p> <p><b>--clear_and_enable_dtpm_txt (Optional)</b> Clears dTPM ownership and activates dTPM/TXT.</p> <p><b>--clear_dtpm (Optional)</b> Clears dTPM ownership and disables dTPM for TPM 1.2. Clears dTPM ownership for TPM 2.0.</p> <p><b>--enable_txt_and_dtpm (Optional)</b> Enables TXT and dTPM.</p> <p><b>--clear_and_enable_dtpm (Optional)</b> Clears dTPM ownership, disables dTPM (for TPM 1.2 only) and activates dTPM.</p> <p><b>--disable_dtpm (Optional)</b> Disables dTPM.</p> <p><b>--disable_txt (Optional)</b> Disables TXT.</p> <p><b>--provision (Optional)</b> Launches the trusted platform module provision procedure.</p> <p><b>--table_default (Optional)</b> Uses the default TPM provision table.</p> <p><b>--table &lt;table name&gt; (Optional)</b> Uses the given customized TPM provision table file.</p>



	<p>.</p> <p><b>--post_complete (Optional)</b>  Waits for the managed system's POST to complete after rebooting.</p>
GetCpuERoTInfo	None
UpdateCpuERoT	<p><b>--file &lt;file name&gt;</b>  Updates the CPU ERoT with the given FW image file.</p> <p><b>--individually</b>  Updates each CPU ERoT with corresponding configuration file individually.</p>
CpuERotManage	<p><b>--action &lt;action&gt;</b>  Sets action to:  1 = GetInfo  2 = UpdateGolden  3 = Recover</p>
FpgaRotManage	<p><b>--action &lt;action&gt;</b>  Sets action to:  1 = GetInfo  2 = UpdateGolden</p>
GetGpuERoTInfo	None
GetSPDMInfo	<p><b>--item &lt;item_name&gt;</b>  Prints the measurements from the specified item.  Item_name:  1 = CPU  2 = GPU</p> <p><b>--showall (Optional)</b>  Prints all measurements.</p>
CmmRotManage	<p><b>--action &lt;action&gt;</b>  Sets action to:  1 = GetInfo  2 = UpdateGolden  3 = Recover  4 = DownloadEvidence</p> <p><b>--file &lt;file name&gt; (Optional)</b></p>

	<p>Works with the --action DownloadEvidence option and saves the CMM evidence to a file.</p> <p><b>--overwrite (Optional)</b> Works with the --action DownloadEvidence option and overwrites the output file.</p> <p><b>--redfish (Optional)</b> Enables pure Redfish support.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 4.5.20. MCU Management

MCU Management	
Commands	Long Options
GetMotherboardMcuInfo	<p><b>-I Redfish_HI (Optional)</b> Uses Redfish Host Interface to query the firmware information. (Only in-band usage is supported.)</p>
UpdateMotherboardMcu	<p><b>--file &lt;file name&gt;</b> Updates the motherboard MCU with the given image file.</p> <p><b>--reboot</b> Forces the managed system to reboot or power up after operation.</p> <p><b>-I Redfish_HI (Optional)</b> Uses Redfish Host Interface to query the firmware information. (Only in-band usage is supported.)</p> <p><b>--post_complete (Optional)</b> Waits for the managed system POST to complete after reboot.</p>



### 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 SAA, use either the relative path method, e.g., ./saa or absolute path method, e.g., /opt/saa\_x.x.x\_Linux\_x64/saa 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 be 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 5 Managing Systems.
  - When a command is executed, it will be recorded in saa.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/SAA” 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 saa 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.
- 

## 4.6. SAA Logs

While SAA 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 an SAA command, the executed command with options from the console will be automatically logged to an saa.log file. 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 SAA 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 an SAA 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 command execution process. The severity levels rank from 0 to 6. 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 to the curl library. With a functional category tag, the journal can be filtered quickly, and issues identified efficiently. By default, this journal is disabled (severity level 0) and it can be enabled by --journal\_level option (higher priority) or .saarc configuration (lower priority). Similarly, this journal will be created at the user home directory by default. In addition, if the output path is assigned in --journal\_path option (higher priority) or .saarc configuration (lower priority), the output path will be replaced.

Types of logs/ properties	Activation	Output path priorities
---------------------------	------------	------------------------

Command usage history	Always activated	<ol style="list-style-type: none"> <li>1. Defined by the option --journal_path. The log exists inside the "History" subfolder in the folder path defined by the option.--journal_path.</li> <li>2. "/var/log/supermicro/SAA".</li> <li>3. \$PWD in Linux or %cd% in Windows.</li> </ol>
Critical error log	Always activated	<ol style="list-style-type: none"> <li>1. Defined by the option --journal_path. The log exists inside the "Critical" subfolder in the folder path defined by the option. --journal_path.</li> <li>2. /var/log/supermicro/SAA.</li> <li>3. \$PWD in Linux or %cd% in Windows.</li> </ol>
Multiple system log	Always activated	<ol style="list-style-type: none"> <li>1. Defined by the option --journal_path. The log exists inside the "Multiple" subfolder in the folder path defined by the option. --journal_path.</li> <li>2. /var/log/supermicro/SAA.</li> <li>3. The same directory as multiple list file.</li> </ol>
Command execution journal	Activated by configuration	<ol style="list-style-type: none"> <li>1. Defined by the option --journal_path. The log exists in the folder path defined by the option. --journal_path.</li> <li>2. Defined by .saarc in the home directory.</li> <li>3. ~/journal/supermicro/saa/ in Linux or</li> </ol>

		%HomePath%\journals\supermicro\saa\ in Windows.
--	--	-------------------------------------------------

## 4.7. XML File Format

### 4.7.1. 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>
```

---

```
</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 conflict in the XML file, SAA 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.

---

## 4.7.2. BMC Configuration XML File Format

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

```
<xml version="1.0">
<BmcCfg>
 <!--You can remove unnecessary elements so that-->
 <!--their values will not be changed after update-->
 <StdCfg Action="None">
 <!--Supported Action:None/Change-->
```



```

<!--Standard BMC configuration tables-->
<FRU Action="Change">
 <!--Supported Action:None/Change-->
 <Configuration>
 <!--Configuration for FRU data-->
 <BoardMfgName>Supermicro</BoardMfgName>
 <!--string value, 0~16 characters-->
 </Configuration>
</FRU>
</StdCfg>
<OemCfg Action="Change">
 <!--Supported Action:None/Change-->
 <!--OEM BMC configuration tables-->
 <ServiceEnabling Action="Change">
 <!--Supported Action:None/Change-->
 <Configuration>
 <!--Configuration for ServiceEnabling-->
 <HTTP>Enable</HTTP>
 <!--Enable/Disable-->
 </Configuration>
 </ServiceEnabling>
</OemCfg>
</BmcCfg>

```

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

---

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

#### 4.7.2.1 Pure Redfish LAN Table in BMC Configuration

If the LAN version of Redfish API is greater than or equal to 1.6.3, SAA will support pure Redfish LAN table in BMC configuration. To check LAN version of Redfish API, please use Redfish API (/redfish/v1/Managers/1/EthernetInterfaces/1) with HTTP method "GET" and find the "@odata.type" field in the response data. The LAN version of Redfish API is 1.6.3 as the following example.

```
@odata.type : "#EthernetInterface.v1_6_3.EthernetInterface"
```

Here are the XPath differences between IPMI LAN table and pure Redfish LAN table in BMC configuration.

- General setting

IPMI LAN table	Pure Redfish LAN table
/BmcCfg/OemCfg/LAN/Configuration/LanMode	/BmcCfg/OemCfg/LAN/Configuration/LanInterface
/BmcCfg/OemCfg/LAN/Configuration/ShareLan	/BmcCfg/OemCfg/LAN/Configuration/LanInterface
/BmcCfg/OemCfg/LAN/Configuration/MacAddress	/BmcCfg/OemCfg/LAN/Information/MacAddress
/BmcCfg/OemCfg/LAN/Configuration/VLAN_Enable	/BmcCfg/OemCfg/LAN/Configuration/VLANEnable
/BmcCfg/OemCfg/LAN/Configuration/VLAN_ID	/BmcCfg/OemCfg/LAN/Configuration/VLANId

- IPv4 setting

IPMI LAN table	Pure Redfish LAN table
/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/IPSrc	/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/DHCPEnabled
/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/IPAddr	/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/Address
/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/DefaultGateWayAddr	/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/Gateway
/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/DNSAddr	/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/IPv4StaticNameServer1
/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/DNSAddr2	/BmcCfg/OemCfg/LAN/Configuration/IPv4/Configuration/IPv4StaticNameServer2

- IPv6 setting

IPMI LAN table	Pure Redfish LAN table
/BmcCfg/OemCfg/LAN/Configuration/DynamicIPv6/Configuration/AutoConfiguration	/BmcCfg/OemCfg/LAN/Configuration/IPv6/Configuration/DynamicIPv6/Configuration/IPv6AutoConfigEnabled
/BmcCfg/OemCfg/LAN/Configuration/DynamicIPv6/Configuration/DHCPv6Mode	/BmcCfg/OemCfg/LAN/Configuration/IPv6/Configuration/DynamicIPv6/Configuration/OperatingMode
/BmcCfg/OemCfg/LAN/Configuration/StaticIPv6/Configuration/DNSv6Mode	/BmcCfg/OemCfg/LAN/Configuration/IPv6/Configuration/IPv6UseDNSServers
/BmcCfg/OemCfg/LAN/Configuration/StaticIPv6/Configuration/IPv6StaticNameServer	/BmcCfg/OemCfg/LAN/Configuration/IPv6/Configuration/IPv6StaticNameServer1

**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.

### 4.7.3. 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 .saarc
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, SAA 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, SAA 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.
- 

#### 4.7.4. 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.



**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.
- 

#### 4.7.5. 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 “RAIDCfgr.” <RAIDCfgr> and </RAIDCfgr> 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.

```
<?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-->
 1
 <!--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>
```

---

#### 4.7.6. Format of the VROC Configuration XML File Format

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>

#### 4.7.7. 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>
 <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-->
 </NodeB>
 </Information>
 </TwinProInfo>
</TwinProCfg>
```

```

 <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-->
 <BpnId>35</BpnId>
 <!--BPN ID-->
 <TwinType>A7</TwinType>
 <!--TwinType-->
 <MCU1Version>0.12</MCU1Version>
 <!--MCU1 Version-->
 <MCU2Version>0.00</MCU2Version>
 <!--MCU2 Version-->
 </Information>
 <Configuration>
 <ConfigId>2</ConfigId>
 <!--Config ID-->
 <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 .
-

---

## 4.7.8. 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>
 <!-- SuperServer Automation Assistant 1.0.0 (2023/08/16)-->
 <!--File generated at 2023-08-17_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® Ethernet
Controller X550(MAC:3cecefc33c6)</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® Ethernet
Controller X550(MAC:3cecefc33c6)</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® Ethernet
Controller X550(MAC:3cecefc33c6)</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® Ethernet
Controller X550(MAC:3cecefc33c6)</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® Ethernet
Controller X550(MAC:3cecefc33c6)</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® Ethernet
Controller X550(MAC:3cecfcb33c6)</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® Ethernet
Controller X550(MAC:3cecfcb33c6)</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® Ethernet Controller X550(MAC:3cecfcb33c6)" 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® Ethernet
Controller X550(MAC:3cecfcb33c6)</Option>
 <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>

```

```

 <Option>Disabled</Option>
 </AvailableOptions>
 <DefaultOption>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefc33c6)</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® Ethernet
Controller X550(MAC:3cecefc33c6)</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® Ethernet Controller X550(MAC:3cecefc33c7)" type="Option">

```

```

 <Information>
 <AvailableOptions>
 <Option>(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet Controller
X550(MAC:3cecefc33c6)</Option>
 <Option>(B4/D0/F1) UEFI PXE IPv4 Intel® Ethernet Controller
X550(MAC:3cecefc33c7)</Option>
 <Option>Disabled</Option>
 </AvailableOptions>
 <DefaultOption>(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet Controller
X550(MAC:3cecefc33c6)</DefaultOption>
 </Information>
 </Setting>
 <Setting name="UEFINetwork #2" selectedOption="(B4/D0/F0) UEFI PXE IPv4
Intel® Ethernet Controller X550(MAC:3cecefc33c6)" type="Option">
 <Information>
 <AvailableOptions>
 <Option>(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet Controller
X550(MAC:3cecefc33c6)</Option>
 <Option>(B4/D0/F1) UEFI PXE IPv4 Intel® Ethernet Controller
X550(MAC:3cecefc33c7)</Option>
 <Option>Disabled</Option>
 </AvailableOptions>
 <DefaultOption>(B4/D0/F1) UEFI PXE IPv4 Intel® Ethernet Controller
X550(MAC:3cecefc33c7)</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® Ethernet Controller X550(MAC:3cecefc33c6)" 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 UEFI Network 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.
- 

## 4.8. Text File Format

### 4.8.1. DMI Information Text 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 SAA according to the BIOS of the managed system for DMI version control.
- 

## 4.9. TUI

SAA supports a text-based user interface (TUI) to make editing of the settings more user-friendly, provide nice visibility, and offer an intuitive and lower learning curve. System configurations can be easily rendered with TUI-like BIOS configurations. It supports Linux, Windows and FreeBSD operating systems. 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**

SAA 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.

#### 4.9.1. TUI General Reminders

Note the following information before using TUI.

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

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

- After you finish using TUI, your original terminal settings will be automatically restored. If restoration fails, locate and run the shell script “restore\_terminal\_config.sh” under the current working directory. The execution command 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 a local terminal with a vt driver (default driver after FreeBSD 11), SAA changes the font to tui.fnt when entering TUI and to **default font** when exiting TUI. You can rename or remove the file ExternalData/tui.fnt to disable this behavior.
- External/tui.fnt is converted from terminus-u12n.bdf by vtfontcvt, check Appendix D for the license.

## 4.9.2. BIOS TUI Configuration

### 4.9.2.1. TUI Display

SAA with TUI simulates a BIOS setup design and its display dimension is set to 30 rows by 100 columns. If SAA fails to resize the terminal with the current terminal settings, it will try to change font type and font size for optimal 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 5.6.3 Getting Current BIOS Settings.
- Some settings and requirements may vary on different BIOS systems where TUI is run.

### 4.9.2.2. How to Use

- **Using Arrow Keys**

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

```
SAA BIOS configuration TUI - Copyright (C) 2023 Super Micro Computer, Inc.
Main Advanced Event Logs Security SMCi KMIP MAIN SMCi HTTP BOOT MAIN Boot

Supermicro X12SPA-TF
BIOS Version 1.1
Build Date 06/21/2021
CPLD Version F0.09.46

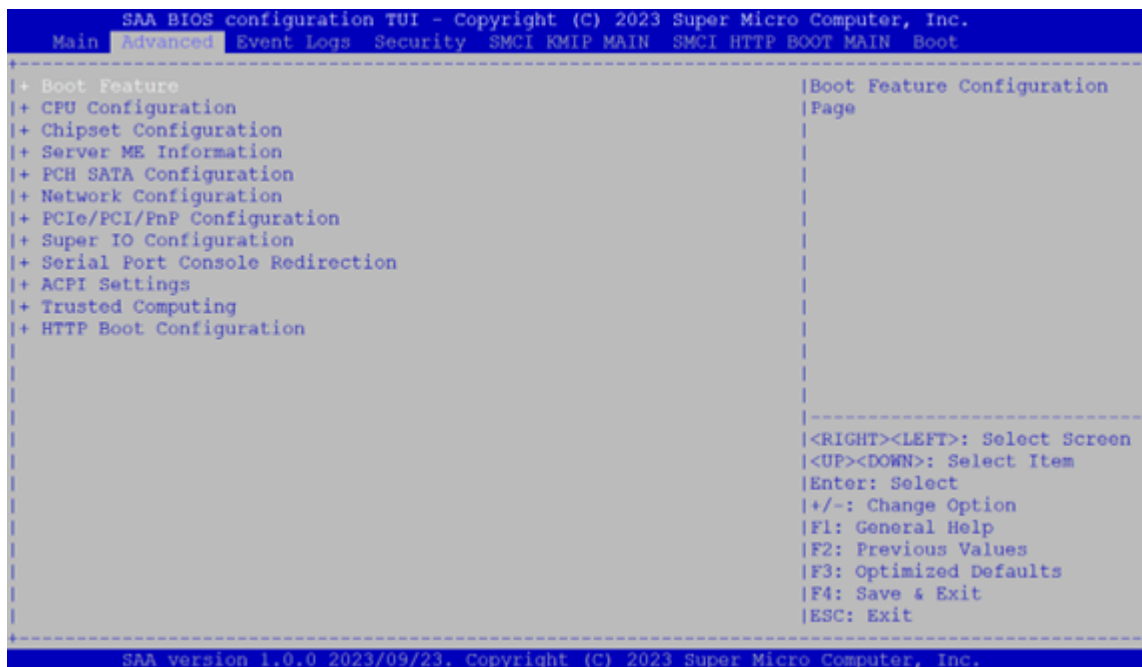
Memory Information
Total Memory 32768 MB

|<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 |

SAA version 1.0.0 2023/09/23. Copyright (C) 2023 Super Micro Computer, Inc.
```

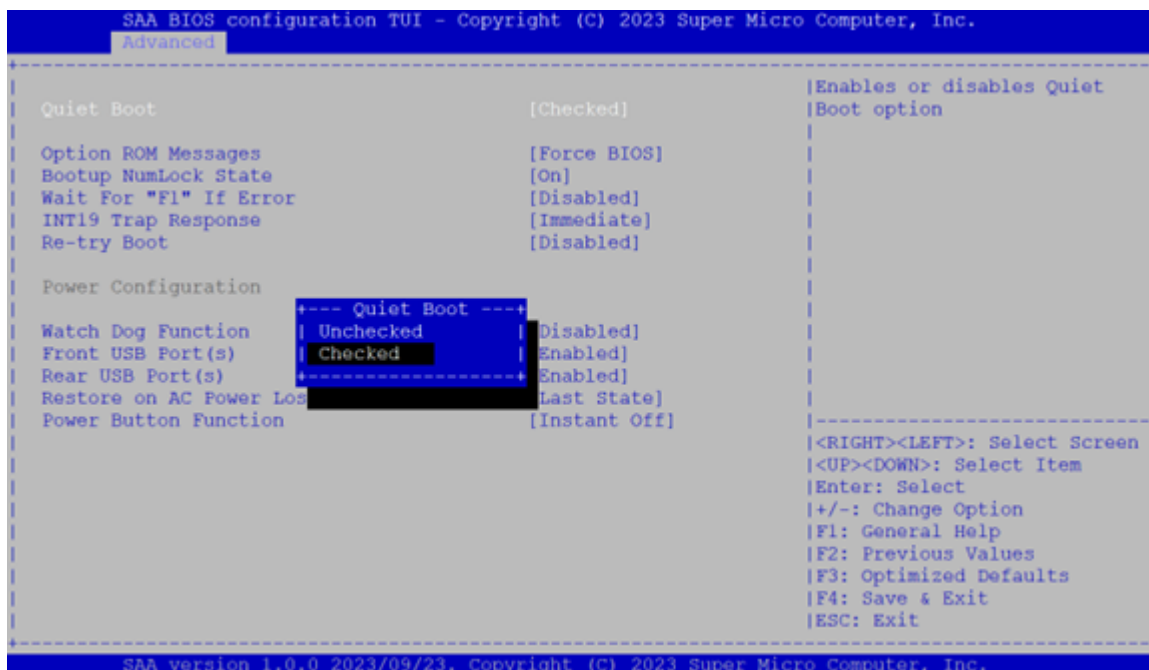
- **Setting Values**

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.



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

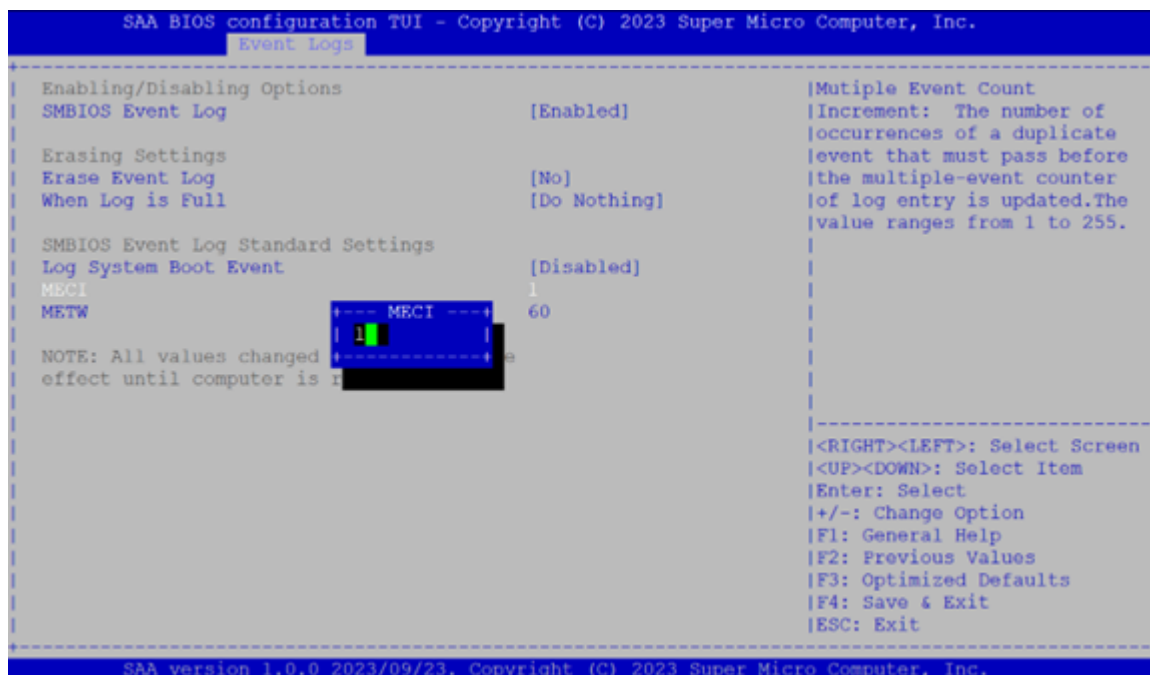
Some functions are allowed to be enabled or disabled. To change the setting, press the **<Enter>** key to call up a dialog box. Press the **<UP>** and **<DOWN>** arrow keys to make a selection. To disable a function, select **Unchecked**. To enable a function, select **Checked**.



- **Setting Numeric Values**

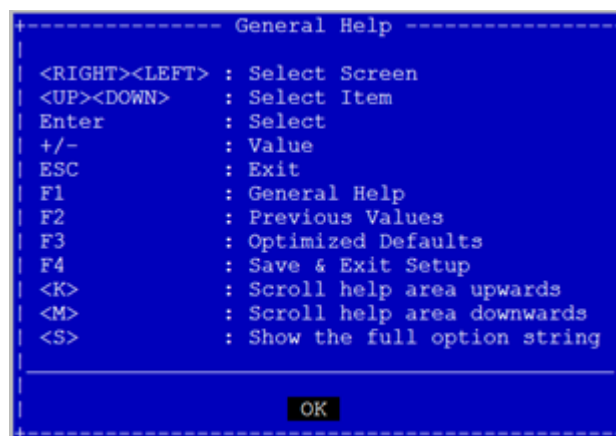
A value may be limited due to the BIOS. You can press the number keys to enter

the desired value or press the <+> and <-> keys to adjust your value within the range. If an input value is incorrect, a warning message appears on screen.



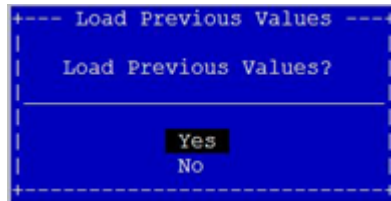
#### 4.9.2.3. Getting General Help

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



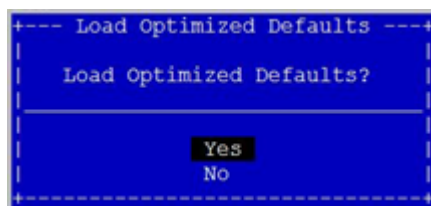
#### 4.9.2.4. Loading Previous Values

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



#### 4.9.2.5. Loading Optimized Values

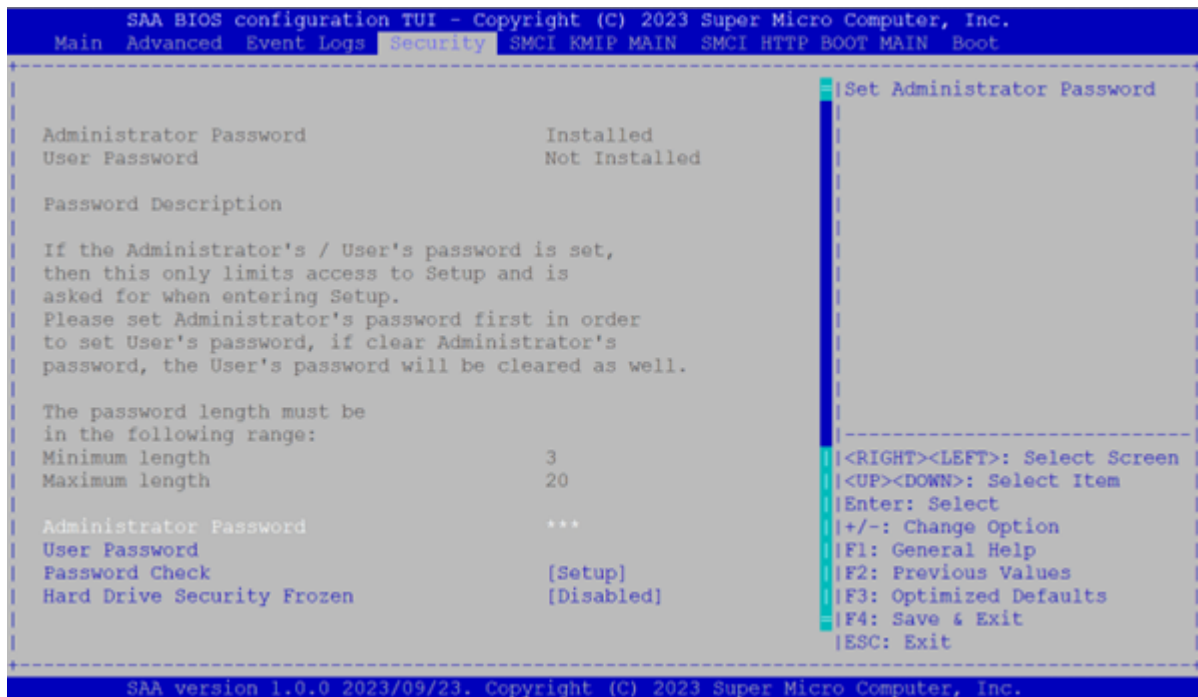
To return all configurations to the default values, press the **<F3>** key. A message appears for confirmation.



#### 4.9.2.6. 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).



#### 4.9.2.7. Exiting the TUI

Two methods are available to exit the SAA 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 from the root menu. You will be returned to the previous menu when you press the **<ESC>** key in submenus.



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



## 5.1. License Management

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

- | Single System    |                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------|
| OOB              | saa -i <IP or host name> -u <username> -p <password> -c<br>ActivateProductKey [--key <nodeproductkey>   --key_file <file name>] |
| In-Band          | saa [-I Redfish_HI -u <username> -p <password>] -c<br>ActivateProductKey [--key <nodeproductkey>   --key_file <file name>]      |
| Multiple Systems |                                                                                                                                 |
| OOB              | saa -l < system list file > [-u <username> -p <password>] -c<br>ActivateProductKey                                              |

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
ActivateProductKey --key '{"ProductKey":{"Node":
{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111111222222222222
```





```
SList.txt:
192.168.34.56
192.168.34.57 ADMIN1 PASSWORD1
```

For the first managed system 192.168.34.56, SAA applies -u ADMIN and -p PASSWORD to the command line and the node product key 1111-1111-1111-1111-1111 to Execute the “ActivateProductKey” command. By contrast, for the second managed system 192.168.34.57, SAA 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 4.4.1.3 Screen Output and 4.4.1.4 Log Output.

**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 Node Product Keys from Supermicro and follow the instructions on the website to load the device driver.

## 5.1.2. Querying the Node Product Keys

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c QueryProductKey
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c QueryProductKey
Multiple Systems	

---

OOB	saa -l < system list file > [-u <username> -p <password>] -c QueryProductKey
-----	------------------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
QueryProductKey
```

**In-Band:**

```
[SAA_HOME]# ./saa -c QueryProductKey
```

```
[SAA_HOME]# ./saa -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

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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.

---

### 5.1.3. Getting and Activating Intel On Demand

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<sup>1</sup> (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.

<sup>1</sup> Downloading DCL (Dear Customer Letter) requires an Intel® RDC (Resource & Documentation Center) account.

#### 5.1.3.1. CpuOnDemand Flow

1. Ensure your CPU<sup>2</sup> is compatible with IOD and run the GetHwInfo 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®.

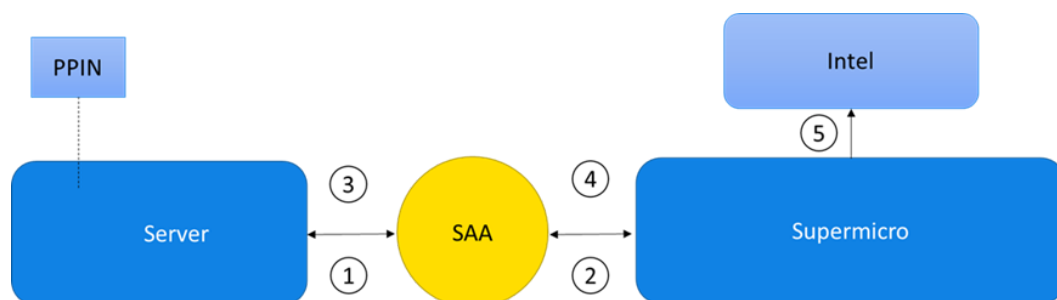


Figure 1 - CpuOnDemand Flow

<sup>2</sup> For On Demand Capabilities-supported CPU SKUs, please contact your sales representative.

SKU Type	Intel MMID	Product Short Name	Intel On Demand Product Suite
XCC	99AV1T	CSS4	<b>Communications &amp; Storage Suite 4</b> QAT 4 Devices DLB 4 Devices DSA 4 Devices
XCC	99AV1V	AMS4	<b>Analytics Suite 4</b> IAX 4 Devices DSA 4 Devices
MCC	99AV1Z	CSS2	<b>Communications &amp; Storage Suite 2</b> QAT 2 Devices DLB 2 Devices
MCC	99AV1R	AMS1	<b>Analytics Suite 1</b> IAX 1 Devices
ALL	99AV1P	SGX512	<b>SGX 512GB</b>

Table 2 - Intel SPR CPU IOD-Supported product names and short names.

#### 5.1.3.2. 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 for a single system:

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CpuOnDemand [--action GetHwInfo] [--cpu_id <cpu_socket_id>] [--file < hw_id_file_name>] [--overwrite]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c CpuOnDemand [--action GetHwInfo] [--cpu_id <cpu_socket_id>] [--file < hw_id_file_name>] [--overwrite]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CpuOnDemand [--action GetHwInfo] [--file < mlist_hw_id_file_name>] [--overwrite]]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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.**

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

```
Hardware type | Index | ID type | Hardware ID | Vendor | SDSi
Enabled
CPU | 0 | PPIN | AABBCDD00112233 | GenuineIntel | YES
File "hwidfile.txt" is created.
```

The format of "hwidfile.txt" is <BMC\_MAC>;<CPU\_ID>;<PPIN> as an example 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:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -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
```

The content of "hwidfile.txt" contains the following information:

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

## 2. Syntax of GetOnDemandState:

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CpuOnDemand --action GetOnDemandState [--cpu_id <cpu_socket_id>   --hw_id <hw_id>   --hw_id_file <hw_id_file_name>] [--v][--squash] [--file <StateReport> [--overwrite]]   --plain_text ]
In-Band	saa -l 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>] [--v][--squash] [--file <StateReport> [--overwrite]]   --plain_text
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CpuOnDemand --action GetOnDemandState [--v][--squash] [--file <StateReport>] [--overwrite]]   --plain_text ]

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:

**00B:**

a. [SAA\_HOME]# ./saa -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. [SAA\_HOME]# ./saa -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","stateCer
tificate":
{"pendingCapabilityActivationPayloadCount":0,"value":"AaaaaBbbbbbCcccc"}]}
,"objectId":"496E74656C5F5F5352","syntaxVersion":"1.0","timestamp":"2022-
09-22T15:28:48+0800"}
```

c. [SAA\_HOME]# ./saa -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 threshold = 2
- SDSi license key auth failure = 0
- SDSi license key auth failure threshold = 2
- SDSi updates available = 2
- SDSi updates threshold = 2

Currently active:
```



- SGX 512 EPC

Active after reboot:

#### In-Band:

```
a. [SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c CpuOnDemand --
action GetOnDemandState --hw_id AABCCDD00112233 --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>.
```

#### Multiple systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -c CpuOnDemand --action GetOnDemandState -
-file mlist_report.txt
```

```
SList.txt:
192.168.34.56 AABCCDD00112233
192.168.34.57 ADMIN1 PASSWORD1 EEFFGGHH00112233
192.168.34.57 ADMIN1 PASSWORD1 EEFFGGHH00445566
```

### 3. Syntax of SetLicenseActivateCode:

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CpuOnDemand --action SetLicenseActivateCode [--lac_file <LAC+.txt>] [--reboot [--post_complete]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c CpuOnDemand --action SetLicenseActivateCode [--lac_file <LAC+.txt>] [--reboot]
Multiple Systems	
OOB	saa -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 2 = GetOnDemandState.

**Format 1:** BMC\_IP\_or\_HostName PPIN

**Format 2:** BMC\_IP\_or\_HostName Username Password PPIN

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p ADMIN -c CpuOnDemand --
action SetLicenseActivateCode --lac_file LAC+_ AABCCDD00112233.txt --
reboot
```

The format of "LAC+\_ AABCCDD00112233.txt" is "<PPIN>;<LAC+ structure>" as an example below:

```
AABCCDD00112233;{"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:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c CpuOnDemand --action
SetLicenseActivateCode --lac_file LAC+_AABCCDD00112233.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:

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c CpuOnDemand --action EnablePPIN --reboot [--post_complete]</code>
In-Band	<code>saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c CpuOnDemand --action EnablePPIN --reboot [--post_complete]</code>
Multiple Systems	
OOB	<code>saa -I &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c CpuOnDemand --action EnablePPIN --reboot [--post_complete]</code>

The format of the system list file is the same as that explained in action 1 = GetHwInfo.

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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

```

---

### In-band :

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

## 5.2. Health Management

### 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 SAA “UpdateBmc” command.
- To update the BIOS in the managed system to support OOB functions, you can use the SAA “UpdateBios” command (either in-band or OOB) to flash BIOS even when BIOS does not support OOB functions. For details, see 5.2.2 Updating the BIOS Firmware Image. 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CheckOOBSupport
In-Band	saa -c CheckOOBSupport
Multiple Systems	

OOB	saa -l < system list file > [-u <username> -p <password>] -c CheckOOBSupport
-----	---------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
CheckOOBSupport
```

#### In-Band:

```
[SAA_HOME]# ./saa -c AlertManage --action listMessage --message_type
Snmpv1
```

#### Multiple systems OOB:

```
[SAA_HOME]# ./saa -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.

#### The console output contains the following information.

```
[KEY]
Node Product Key Format.....JSON
Node Product Key Activated.....SFT-DCMS-SINGLE
 SFT-DCMS-SVC-KEY Activated...No
 SFT-SDDC-SINGLE Activated....No
Feature Toggled On.....Yes

[BMC]
BMC FW Version.....01.02.18
IPMI Version.....2.0
Manufacturer ID.....7C 2A 00
Product ID.....52 1C 00
Auxiliary Firmware Revision.....18 01 00 00
```

```

BMC Supports OOB BIOS Config....Yes
BMC Supports OOB DMI Edit.....Yes

[BIOS]
Board ID.....1C52
BIOS Build Date.....2023/10/19
BIOS Version.....2.0
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. The add-on devices are displayed by the riser cards to which they are connected.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CheckAssetInfo
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CheckAssetInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CheckAssetInfo
```

**Multiple OOB:**

```
saa -l < system list file > [-u <username> -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.

**The console output for a single system contains the following information.**

```
System
=====
 Product Name:
 Product PartModel Number:
 Version: 0123456789
 Serial Number:
 UUID: 00000000-0000-0000-0000-AC1F6B0FEA62

Baseboard
=====
 Product Name: H11DSU-iN
 Version: 0123456789
 Serial Number: 0123456789

CPU
===
 [CPU(1)]
 Processor Architecture: x86
 Manufacturer: Advanced Micro Devices, Inc.
 Version: AMD EPYC 7551 32-Core Processor
 Family: AMD Zen Processor Family
 CPU ID: 12 0f 80 00 ff fb 8b 17
 Current Speed: 2000 MHz
 Total Cores: 32
 Enabled Cores: 32
 Thread Count: 64
 TDP Watts: 0
 [CPU(2)]
 Processor Architecture: x86
 Manufacturer: Advanced Micro Devices, Inc.
 Version: AMD EPYC 7551 32-Core Processor
 Family: AMD Zen Processor Family
 CPU ID: 12 0f 80 00 ff fb 8b 17
 Current Speed: 2000 MHz
 Total Cores: 32
 Enabled Cores: 32
 Thread Count: 64
 TDP Watts: 0

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)] N/A
[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)]
```

```
Locator: P2-DIMMA2
Memory Type:
Manufacturer: Samsung
Manufacturing Date (YY/WW): 16/25
Device Type: DDR4
Serial Number: 32AEC18B
Part Number: M393A1G40DB0-CPB
Data Width: 64 bits
Bus Width: 72 bits
Current Speed: 2133 MT/s
Size: 8192 MB
Error Correction: MultiBitECC
Module Type: RDIMM
Rank: 1
```

```
[MEM(19)] N/A
[MEM(20)] N/A
[MEM(21)] N/A
[MEM(22)] N/A
[MEM(23)] N/A
[MEM(24)] N/A
[MEM(25)] N/A
[MEM(26)] N/A
[MEM(27)] N/A
[MEM(28)] N/A
[MEM(29)] N/A
[MEM(30)] N/A
[MEM(31)] N/A
[MEM(32)] N/A
```

#### Add-on Network Interface

=====

```
[[[SXB3 (Riser)]]]
[[Onboard]]
[NIC(1)]
```

Device Class: Network controller



---

```
Device Subclass: Ethernet controller
Vendor: (ID:8086)
Subvendor: (ID:15D9)
Device Name: (ID:1528)
Subsystem Name: (ID:0847)
Serial Number: 0A182S021066
Part Number: AOC-UR-i4XT
MAC Address1: AC1F6B0FEA62
Current Speed1: 1000Mb/s
MAC Address2: AC1F6B0FEA63
Current Speed2: 0Mb/s
MAC Address3: AC1F6B0FEA64
Current Speed3: 0Mb/s
MAC Address4: AC1F6B0FEA65
Current Speed4: 0Mb/s
Slot Number: Onboard
Slot Designation: SXB3
```

#### Add-on PCI Device

=====

```
[[[SXB3 (Riser)]]]
[[Onboard]]
[Device(1)]
```

```
Device Class: Network controller
Device Subclass: Ethernet controller
Vendor: (ID:8086)
Subvendor: (ID:15D9)
Device Name: (ID:1528)
Subsystem Name: (ID:0847)
Slot Number: Onboard
Slot Designation: SXB3
```

#### Onboard Network Interface

=====

N/A

#### Onboard PCI Device

=====

```
[Device(1)]
```

```
Device Class: Display controller
Device Subclass: VGA-compatible controller
Vendor: (ID:1A03)
Subvendor: (ID:15D9)
Device Name: (ID:2000)
Subsystem Name: (ID:0963)
```

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

```
[Device(2)]
 Device Class: Serial bus controller
 Device Subclass: Universal Serial Bus(USB) Host Controller following
the Intel eXtensible Host Controller Interface (xHCI) Specification
 Vendor: (ID:1B21)
 Subvendor: (ID:1B21)
 Device Name: (ID:1142)
 Subsystem Name: (ID:1142)

 Device Status of Other1: Enabled
 Device Type: Other
 Reference Designation of Other1: ASMedia USB 3.1
```

```
[Device(3)]
 Device Class: Serial bus controller
 Device Subclass: Universal Serial Bus(USB) Host Controller following
the Intel eXtensible Host Controller Interface (xHCI) Specification
 Vendor: (ID:1B21)
 Subvendor: (ID:1B21)
 Device Name: (ID:1142)
 Subsystem Name: (ID:1142)

 Device Status of Other2: Enabled
 Device Type: Other
 Reference Designation of Other2: ASMedia USB 3.1
```

#### System Network Interface

=====

```
[LAN(1)]
 MAC Address: AC1F6B0FEA62
 IPv4 Address: 10.146.172.29
 IPv6 Address:
2001:db8:0:f102:4195:1c5:4d3:dd25,2001:db8::536c:93e5:b88f:9796,fe80::5e30:66bf:a
ca9:42f
 Current Speed: 1000Mb/s
[LAN(2)]
 MAC Address: AC1F6B0FEA63
 IPv4 Address: N/A
 IPv6 Address: N/A
 Current Speed: 0Mb/s
[LAN(3)]
 MAC Address: AC1F6B0FEA64
 IPv4 Address: N/A
 IPv6 Address: N/A
 Current Speed: 0Mb/s
[LAN(4)]
 MAC Address: AC1F6B0FEA65
 IPv4 Address: N/A
 IPv6 Address: N/A
 Current Speed: 0Mb/s
```

---

#### IPMI Network Interface

=====

[IPMI]

MAC Address: 0025905E9153

#### Power Supplies

=====

[(PSU1)]

Model: PWS-2K05A-1R

Serial Number: P2K5ACI49CT0013

Type: AC

Capacity Watts: 2000 W

Firmware Version: 1.2

Sensor Number: 196



#### Notes:

- 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, their device information will be listed in the add-on card section and under the label "Onboard."
- 

### 5.2.3. Checking Sensor Data

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



#### Notes:

- Supported sensors vary between 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."
- 

Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c CheckSensorData [--action <action> [--sdr_id <id>] [--sdr_major_version <version> --sdr_minor_version <version>]] [--showall]
In-Band	saa -c CheckSensorData [--action <action> [--sdr_id <id>] [--sdr_major_version <version> --sdr_minor_version <version>]] [--showall]
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c CheckSensorData [--action <action> [--sdr_id <id>] [--sdr_major_version <version> --sdr_minor_version <version>]] [--showall]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
CheckSensorData
```

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

```
Status | (#)Sensor | Reading | Low Limit | High Limit |
-----|-----|-----|-----|-----|
OK | (4) CPU Temp | 41C/106F | 5C/41F | 104C/219F |
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
CheckSensorData --action Show --showall
```

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

```
Status | (#)Sensor | Reading | Low NR | Low CT | Low
NC | High NC | High CT | High NR |
-----|-----|-----|-----|-----|
--- | -----|-----|-----|
OK | (4) CPU Temp | 42C/108F | 5C/41F | 5C/41F |
10C/50F | 99C/210F | 104C/219F | 104C/219F |
```

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
CheckSensorData -- action Del --sdr_id 4
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
CheckSensorData -- action GetVer
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
CheckSensorData -- action SetVer --sdr_major_version 0 --
sdr_minor_version 255
```

### Multiple Systems OOB:

```
[SAA_HOME]#./saa -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 BIOS and BMC capabilities of the managed system will be shown in the "Execution Message" section in the created log file.

## 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.

---

Single System
---------------

---

OOB	saa -i <IP or host name> -u <username> -p <password> -c CheckSystemUtilization
<b>Multiple Systems</b>	
OOB	saa -l <system list file> -u <username> -p <password> -c CheckSystemUtilization

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
CheckSystemUtilization
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -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.

**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 be displayed.
- 

### 5.2.5. Monitoring the Host with 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ServiceCalls [--file <servicecalls XML file>]
In-Band	saa -c ServiceCalls [--file <servicecalls XML file>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c ServiceCalls [--file <servicecalls XML file>]

Example:

**OOB:**

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

**In-Band:**

```
./saa -c ServiceCalls --file servicecalls_sample.xml
```

**Multiple system OOB:**



---

```
[SAA_HOME]# ./saa -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.

### 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 SAA 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 SAA. SAA 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 on 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 recipient’s e-mail address (“RecipientEmail”) is genuine 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](mailto: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: b7f45efc-eb58-84d7-667d-4be63dab2a4a] - SSAA Service Calls Alerts "154" has some problems (Critical: 2 Warning: 0 Information: 0 ) and 0 recovered item(s)



Tue 8/28/2023 4:00 PM

Report Suspicious

SAA Service Calls

Host IP: 192.168.20.18

Host System: BMC

Event ID: b7f45efc-eb58-84d7-667d-4be63dab2a4a

Event Source: Critical Super Server 010113.1.30

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 "SAA 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 SAA. 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 CPU Socket#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:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, HDD_OEM, Disk120 SMART failure				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT GH				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT GH				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT EF				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT EF				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT CD				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT CD				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT AB				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, MEM EVENT AB				
[#Recovered from Event ID:96896644-94bb-25db-fcf1-cb6ccd194ea0] CRITICAL, 2020/10/29 20:29:30, CPLD_OEM, PROCHOT F2				
[#Recovered from Event ID:96896644-94bb-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: SMCI  
Address: Test\_Info  
City: Test\_Info  
State/Province: CC  
Zip: 333  
Country: TT  
Contact Person: User, Administrator  
Email: [test\\_mail@supermicro.com](mailto:test_mail@supermicro.com)

The location where the managed system is located.

- **Customer Info:**

[Customer Info]  
Company: SMCI  
Contact Person: User  
Email: [test\\_mail@supermicro.com](mailto:test_mail@supermicro.com)

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 .saarc file. For details, see 4.2 Customizing SAA Configurations. The execution history, including e-mail contents and e-mail sender/recipient information, is saved in a database file for SAA 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:**

- SAA 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SystemPFA [--action <action>] [--reboot [--post_complete]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c SystemPFA {--action <action>} [--reboot]
Multiple Systems	
OOB	saa -I < 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:

### OOB:

```
1. [SAA_HOME]# ./saa -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. [SAA_HOME]# ./saa -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 :**

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

#### **Multiple systems OOB:**

```
[SAA_HOME]# ./saa -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.



#### **Note:**

This command is only available on X13 and later 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c MemoryHealthCheck [--action <action>] [--reboot [--post_complete]]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c MemoryHealthCheck [--action <action>] [--reboot]
Multiple Systems	
OOB	saa -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:

**OOB:**

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

The current memory health checking is Disabled

```
[SAA_HOME]# ./saa -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:**

```
[SAA_HOME]# ./saa -l Redfish_HI -u ADMIN -p PASSWORD -c MemoryHealthCheck --
action Enable --reboot
```

#### **Multiple systems OOB:**

```
[SAA_HOME]# ./saa -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.

## **5.2.8. 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”.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChassisIntrusion --action {Clear   Status}
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c ChassisIntrusion --action {Clear   Status}
Multiple Systems	
OOB	saa -I < system list file > [-u <username> -p <password>] -c ChassisIntrusion --action {Clear   Status}

Example:

#### OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# sudo ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
ChassisIntrusion --action Clear
```

The console output contains the following information.

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

#### Multiple OOB:

---

```
[SAA_HOME]# ./saa -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.

## 5.2.9. Getting Alert Messages

### 5.2.9.1. Setting the Destination for Alert Messages

To receive alert messages, you need to configure the server IP location through BMC. You can use the SAA "SetBmcCfg" command or configure it through the BMC web page. Here's an example of how to configure it through the BMC web page of the current server:

1. Go to the BMC web page of the server.
2. Navigate to the Configuration/Notifications menu and select the Alerts tab.
3. Choose the message notifications that you want to receive and specify the server location.

### 5.2.9.2. Use Alert Sever

In the "SAA" folder, there is a subfolder named "GO\_SNMP", which contains an AlertServer application. AlertServer is a server that includes a basic HTTPS server and an SNMP listener. When starting the AlertServer, it begins to receive messages for SNMPv1, SNMPv3, and Redfish alerts. AlertServer will write the received messages to an SQLite database file in the default or specified path that messages can be read through the SAA AlertManage command.

The "GO\_SNMP" folder contains an SNMP configuration file named "snmp.env". The "snmp.env" file includes the following settings:

Setting Name	Setting Value Sample	Description
UserName	UserName	Sets the name for SnmpV3
AuthenticationProtocol	MD5 SHA SHA224 SHA256 SHA384 SHA512	Sets the Authentication Protocol for SnmpV3
AuthenticationPassphrase	Password	Sets the Authentication Passphrase for SnmpV3
PrivacyProtocol	DES AES AES192 AES256 AES192C AES256C	Sets the Privacy Protocol for SnmpV3
PrivacyPassphrase	Password	Sets the Privacy Passphrase for SnmpV3
db_path	default.db	Set the path for storing alert messages
server_cert	server.cert	Sets the Https server SSL certificate loading path
server_key	server.key	Sets the Https server SSL key loading path
log_level	1 (no log) 2 (simple log) 3 (complete log)	Set Server log level

### 5.2.9.3. Getting Alert Message

Use the “AlertManage” command to get different types of alert messages on the managed system. In addition, a new setting has been added to the SAARC file for configuring the path to the SQLite database file used to read Alert Message.

#### Single System

---

In-Band	saa -c AlertManage --action listmessage --message_type <List of message type>[--after <datetime>] [--before <datetime>][--ip <Sender IP>][--page <Page>] [--limit <limit>]
---------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Example:

#### **In - Band :**

```
[SAA_HOME]# ./saa -c AlertManage --action listMessage --message_type
Snmpv1
```

#### **5.2.9.4. Query Alert Message**

When searching or browsing through specific alert messages, the following example can be referenced.

Example:

```
[SAA_HOME]# ./saa -c AlertManage --action listmessage --message_type
snmpv1 -- after "2022-12-09 19:48:36"
```

```
[SAA_HOME]# ./saa -c AlertManage --action listmessage --message_type
snmpv1 -- before "2022-12-09 19:48:36"
```

To search for SNMPv1 messages after a certain time, the option "--after" can be used, and to look for messages before a certain time, the option "--before" can be used.

```
[SAA_HOME]# ./saa -c AlertManage --action listmessage --message_type
snmpv1 -- after "2022-12-08 19:48:36" --before "2022-12-09 19:48:36"
```

The options "--after" and "--before" can also be combined to search for alert messages between two specific times.

```
[SAA_HOME]# ./saa -c AlertManage --action listmessage --message_type
snmpv1 --ip 192.168.34.56
```

The "--ip" option can be used to search for alert messages that originated from a particular IP address.

---

```
[SAA_HOME]# ./saa -c AlertManage --action listmessage --message_type
snmpv1 -- limit 10 --page 3
```

The AlertManage command is designed to list only 20 alert messages at a time. If there are too many messages, you can use the "--page" option to review the next 20 messages. Additionally, the option "-- limit" can be used to set how many messages can be listed at a time.

```
[SAA_HOME]# ./saa -c AlertManage --action listmessage --message_type 1 --
ip 192.168.34.56 --after "2023-1-1 00:00:00" --before "2023-1-1 14:00:00"
--limit 10 --page 3
```

When using AlertManage, every search option value will be output under the notice title. Additionally, Page Info will list the number of pages that can be navigated to.

**The console output contains the following information.**

```
[Notice]
No matching results with SnmpV1 message
#The searching criteria:
#IP : 192.168.34.56
#timeafter : 2023-1-1 00:00:00
#timebefore : 2023-1-1 14:00:00
[Page Info]
#Total 0 records
```



**Note:** The default values for "--limit" and "--page" are 20 and 1, respectively.

---

#### 5.2.9.5. Send Test Alert

Use the "AlertManage" command with the action "sendTest" .

Syntax:

```
saa <-i | -I Redfish_HI> -u ADMIN -p PASSWORD -c AlertManage --action
sendTest
```

Example:

---

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c AlertManage --
action sendTest
```

**In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c AlertManage --action
sendTest
```



**Note:** The action sendTest only support Redfish\_HI, OOB and multi-OOB.

---

### 5.2.10. Running Super Diagnostics Offline (SDO) Remotely

To run BIOS diagnostic functions remotely, Super Diagnostic Offline (SDO) is required. SDO is a system diagnostic tool that runs in EFI shell that provides the capability to determine the health of a Supermicro server's components. To learn more about SDO, please visit <https://www.supermicro.com/en/solutions/management-software/super-diagnostics-offline>

#### Getting SuperDiag ISO Image

Follow the steps below to download and retrieve the SuperDiag ISO image:

1. Download the zip file "SuperDiag\_x.x.x\_Tyyyymmdd.zip" from <https://www.supermicro.com/en/support/resources/downloadcenter/smsdownload>
2. Unzip "SuperDiag\_x.x.x\_Tyyyymmdd.zip" to create a folder named the "SuperDiag\_x.x.x\_Tyyyymmdd".
3. Locate "ISOForSuperDiag.zip" within the SuperDiag\_x.x.x\_Tyyyymmdd\Diagnose\_Remotely subfolder to get the ISO image "SuperDiag.x.x.x.iso"

#### Creating a SuperDiag pen drive

Follow the steps below to create a SuperDiag pen drive:



1. Download the zip file "SuperDiag\_x.x.x\_Tyyyymmdd.zip" from <https://www.supermicro.com/en/support/resources/downloadcenter/smsdownload>
2. Unzip "SuperDiag\_x.x.x\_Tyyyymmdd.zip" to create a folder named the "SuperDiag\_x.x.x\_Tyyyymmdd".
3. Locate 'USBForSuperDiag.zip' within the 'SuperDiag\_x.x.x\_Tyyyymmdd\Diagnose\_Remotely' subfolder. Unzip the file and copy the extracted contents to a pen drive.

## Running the SuperDiag Command

Use the "SuperDiag" command to run the BIOS diagnostic, download and check diagnostic results. The supported actions are as follows:

### • Starting Diagnostics

Use the "SuperDiag" command with the "--action Start" option to start diagnostics.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SuperDiag --action Start [--file <ISO image>   --image_url <URL of ISO image> [--dev_id <index>]   --usb --index <index>} --reboot
Multiple Systems	
OOB	saa -l <system list file> -c SuperDiag --action Start --file --image_url <URL of ISO image> [--dev_id <index>] --reboot

### • Downloading Diagnostic Results

Use the "SuperDiag" command with the "--action Download" option to download diagnostic results in JSON format.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SuperDiag --action Download --file <results.json> [--overwrite]
In-Band	saa -c SuperDiag --action Download --file <results.json> [--overwrite]
Multiple Systems	

OOB	saa -l <system list file> -c SuperDiag --action Download --file <results.json> [--overwrite]
-----	----------------------------------------------------------------------------------------------

### • Check Diagnostics Results

Use the “SuperDiag” command with the “--action Display” option to check diagnostic results.

Single System	
In-Band	saa -c SuperDiag --action Display --file <results.json> [--type <display type>] [--keyword <keyword>] [--line <number>]

### • Listing the Available Devices for Diagnostics

Use the “SuperDiag” command with the “--action List” option to list all devices available for diagnostics.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SuperDiag --action List --usb
In-Band	saa -c SuperDiag --action List --usb

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SuperDiag --
action Start --file SuperDiag_1.9.0.iso -reboot
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SuperDiag --
action Start --image_url '\2001:db8::1\MySharedPoint\MyFolder\Image.iso'
--dev_id 2 --reboot
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SuperDiag --
action Start --usb --index 3 --reboot
```

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SuperDiag --
action Download --file results.json
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c SuperDiag --action Download --file results.json
```

```
[SAA_HOME]# ./saa -c SuperDiag --action Display --file results.json --
type info --keyword BIOS
```

```
[SAA_HOME]# ./saa -c SuperDiag --action Display --file results.json --
type fail --line 20
```

#### **The console output contains the following information.**

```
System Component Detection:
 RAID Detection:
 Device presence check:
 Result: Aborted
 Backplane Detection:
 Device presence check:
 Result: Aborted
 GPU Detection:
 Device presence check:
 Result: Aborted
CPU Diagnostics:
 CPU #001 - AMD Eng Sample: 100-000000897-03 :
 Brand-string Test:
 Result: Failed
Network Diagnostics:
 Broadcom Ethernet BCM57416/5720L #2:
 Network Connection:
 Result: Aborted
PCIe Diagnostics:
 ASPEED Video AST2600:
```

```
[SAA_HOME]# ./saa -c SuperDiag --action List --usb
```

```
....
3: [sdc1: SCSI Disk]
4: [sda1: SCSI Disk]
5: [sdb1: SCSI Disk]
```

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SuperDiag --action
Start --image_url '\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --
dev_id 2 --reboot
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SuperDiag --action
Download --file results.json
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

### 5.2.10.1. Running Diagnostics in Embedded Mode

Use the “SuperDiag” command with the “--action Start” and “--embedded” options to start diagnostics in embedded mode.

#### • Starting Diagnostics

Use the “SuperDiag” command with the “--action Start --embedded” options to start diagnostics in embedded mode.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SuperDiag --action Start --embedded --reboot
Multiple Systems	
OOB	saa -l <system list file> -c SuperDiag --action Start --embedded -- reboot

#### • Downloading Diagnostic Results

---

Use the “SuperDiag” command with the “--action Download” and “--embedded” options to download embedded diagnostic results in HTML format.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SuperDiag --action Download --embedded --file <results.html> [--overwrite]
In-Band	saa -c SuperDiag --action Download --embedded --file <results.html> [--overwrite]
Multiple Systems	
OOB	saa -l <system list file> -c SuperDiag --action Download --file <results.html> [--overwrite]

#### • Check diagnostics results

For BIOS diagnostics in embedded mode, the downloaded diagnostic result is in HTML format. Please open the HTML file in a browser to check the diagnostics results.



#### Notes:

- SuperDiag with the --action Start option does not support In-Band usage.
  - SuperDiag with the --action Display option does not support OOB usage and multiple system OOB usage.
  - The --action List option can display available hard drives, but the hard drives cannot be used with the --action Start option for diagnostics due to security restrictions.
- 

### 5.2.11. Sending Diag Interrupt

Use the “SendDiagInterrupt” command to send system diagnostic interrupts. This command sends a system diagnostic interrupt (NMI, Non-Maskable Interrupt) hardware interrupt. In practice, this action may result in different behaviors across different operating systems.

<b>Single System</b>
----------------------

OOB	saa -i <IP or host name> -u <username> -p <password> -c SendDiagInterrupt
In-Band	saa -c SendDiagInterrupt
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SendDiagInterrupt

Example:

#### **OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SendDiagInterrupt
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c SendDiagInterrupt
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SendDiagInterrupt
```

```
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.

## **5.2.12. Monitoring CDU Status**

### **5.2.12.1. Getting CDU Information**

Use the “MonitorCDUStatus” command to execute SAA to show the current CDU Web UI Status remotely. With the --file option, the CDU status can be saved into an output file.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c MonitorCDUStatus [--action <GetStatus 1>} [--file <CDUStatus.txt> [--overwrite]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c MonitorCDUStatus [--action <GetStatus 1>} [--file <CDUStatus.txt> [--overwrite]]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c MonitorCDUStatus
--action GetStatus
```

```
[SAA_HOME]# ./saa -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]

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MonitorCDUStatus -
-action GetStatus --file CDUStatus.txt --overwrite
```

```
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

### 5.2.12.2. Setting CDU Alert Setting

Use the “MonitorCDUStatus” command to execute SAA to set CDU alert setting with the CDU\_alert\_setting.json file.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c MonitorCDUStatus --action SetCfg 2 [--file <CDU_alert_setting.json>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c MonitorCDUStatus --action SetCfg 2 [--file <CDU_alert_setting.json>]



---

Example:

**00B:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c MonitorCDUStatus
--action SetCfg --file CDU_alert_setting.json
```

**Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -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.

### 5.2.12.3. JSON File Format of CDU alert setting

A CDU alert setting JSON file format is explained below. The sample file is named as “CDU\_alertsetting\_sample.json” and bundled in the SAA 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 warning 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

### 5.2.13. Managing TAS Functionality

Use the “TasManage” command to execute TAS related actions. Make sure TAS is installed in the managed system before using the command. Please refer to 2.2.1 Installing the TAS Package. The supported actions are as follows:

- **Getting Information on TAS**

Use the “TasManage” command with the “--action GetInfo” option to retrieve information from TAS.

- **Pausing TAS service**

Use the “TasManage” command with the “--action Pause” option to pause TAS service.

- **Resuming TAS service**

Use the “TasManage” command with the “--action Resume” option to resume TAS service.

- **Recollecting TAS data**

Use the “TasManage” command with the “--action Refresh” option to trigger TAS to recollect data.

- **Clearing TAS data**

---

Use the “TasManage” command with the “--action Clear” option to clear the collected TAS data in the BMC.

- **Setting TAS update period**

Use the “TasManage” command with the “--action SetPeriod” option to set the TAS update period in second (between 5 and 60 seconds).

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c TasManage --action <action> [--period <update period>]
In-Band	saa -c TasManage --action <action> [--period <update period>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c TasManage --action <action> [--period <update period>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TasManage --
action GetInfo
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TasManage --
action Pause
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TasManage --
action Resume
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TasManage --
action Refresh
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TasManage --
action Clear
```

**In-Band:**

```
[SAA_HOME]# ./saa -c TasManage --action SetPeriod --period 5
```

---

```
[SAA_HOME]# ./saa -c TasManage --action GetInfo
```

The console output contains the following information.

```
Item | Value

Version | 1.7.0
Build Data | 220503
Protocol Version | 0x01
Status | Stopped
TAS Start Time | Fri Aug 11 22:36:05 2023
Last Update Time | Fri Aug 11 22:45:50 2023
```

#### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TasManage --action
GetInfo
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TasManage --action
Pause
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TasManage --action
Resume
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

### 5.2.14. Checking and Reporting Basic Health Status of the BMC

Use the “CheckSelfTest” command to execute SAA to show the basic status of the BMC system.

<b>Single System</b>
----------------------

OOB	saa -i <IP or host name> -u <username> -p <password> -c CheckSelfTest
In-Band	saa -c CheckSelfTest
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CheckSelfTest

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CheckSelfTest
```

#### In-Band:

```
[SAA_HOME]# ./saa -c CheckSelfTest
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
.....
Self Test is passed
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c CheckSelfTest
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

## 5.2.15. Getting and Setting Hardware Debug Tool Status

Use the “HDTService” command to get or set the hardware debug tool status of the BMC system.

Command Options	Descriptions
--action	Sets action to: 1 = GetHDTStatus 2 = Enable 3 = Disable

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c HDTService --action <action>
In-Band	-I Redfish_HI -u <username> -p <password> -c HDTService --action <action>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c HDTService --action <action>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c HDTService --action GetHDTStatus
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.0.0 (2024/04/02) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
.....
HDT is disabled.
```

**In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c HDTService --action Enable
```

---

```
SuperServer Automation Assistant 1.0.0 (2024/04/02) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
.....
The HDT is set to Enable.
```

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c HDTService --
action Disable
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

If the "Status" field in the execution of the managed system displays "SUCCESS," the console output of the managed system will appear in the "Execution Message" section of the created log file.

## 5.3 System Management

### 5.3.1 Managing FRU Information

#### 5.3.1.1 Getting FRU Information

Use the "GetFruInfo" command to get or dump FRU information from 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.

---

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetFruInfo [--file <filename> --dump [--format <file format>] [--overwrite]] [--dev_id <Device ID>]   [--showall]



In-Band	<code>saa -c GetFruInfo [--file &lt;filename&gt; [--dump [--format &lt;file format&gt;] [--overwrite]   --file_only]] [--dev_id &lt;Device ID&gt;]   [--showall]</code>
<b>Multiple Systems</b>	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c GetFruInfo [--file &lt;filename&gt; --dump [--format &lt;file format&gt;] [--overwrite]] [--dev_id &lt;Device ID&gt;]   [--showall]</code>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetFruInfo --dev_id 1,2
```

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

**The console output contains the following information.**

```
FRU information [Version=00.00]
=====
[CMM Master, ID=1, Size=256 bytes]
 Board mfg. Date/Time (BDT): 2022/08/17 13:49
 Board Manufacturer Name (BM): Supermicro
 Board Product Name (BPN): Chassis Management Module
 Board Serial Number (BS): UD22CS001903
 Board Part Number (BP): MBB-CMM-6
 Board Version (BV):
 Product Manufacturer (PM): Supermicro
 Product Name (PN): Chassis Management Module
 Product Part/Model Number (PPM): MBM-CMM-6
 Product Version (PV): 1.03
 Product Serial Number (PS):
 Product Asset Tag (PAT):

[CMM Middle Plane, ID=2, Size=256 bytes]
 Board mfg. Date/Time (BDT): 2017/08/14 14:32
 Board Manufacturer Name (BM): Supermicro
 Board Product Name (BPN): MidPlane
 Board Serial Number (BS): GB197S006422
 Board Part Number (BP): BPN-SB-J820
 Product Manufacturer (PM): Supermicro
 Product Name (PN): MidPlane
 Product Part/Model Number (PPM): BPN-SB-J820
 Product Version (PV): 1.01A
```

---

```
Product Serial Number (PS): GB197S006422
Product Asset Tag (PAT):
```

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

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetFruInfo --
file dumpedFile --dump --format TEXT --overwrite
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetFruInfo --
file dumpedFile --dump --format BINARY --overwrite
```

**The console output contains the following information.**

```
FRU information [Version=01.01]
=====
[BMC, ID=0, Size=256 bytes]
 Board mfg. Date/Time (BDT): 1996/01/01 00:00
 Board Manufacturer Name (BM):
 Board Product Name (BPN):
 Board Serial Number (BS):
 Board Part Number (BP):
 Product Manufacturer (PM):
 Product Name (PN):
 Product Part/Model Number (PPM):
 Product Version (PV):
 Product Serial Number (PS):
 Product Asset Tag (PAT):

File "dumpedFile" is created
```

**Inband:**

```
[SAA_HOME]# ./saa -c GetFruInfo --file dumpedFile --file_only
```

**The console output contains the following information.**

```
Chassis Type (CT): 01
Chassis Part Number (CP):
Chassis Serial Number (CS):
Board mfg. Date/Time (BDT): 2021/08/30 18:01
Board Manufacturer Name (BM): Supermicro
Board Product Name (BPN):
Board Serial Number (BS): WM218S011157
```

---

```
Board Part Number (BP):
Product Manufacturer (PM):
Product Name (PN):
Product Part/Model Number (PPM):
Product Version (PV):
Product Serial Number (PS):
Product Asset Tag (PAT):
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetFruInfo --file
dumpedFile --dump
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetFruInfo --
dev_id 1,2
```

```
[SAA_HOME]# ./saa -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, SAA will create dumpedFile.192.168.34.56 and dumpedFile.192.168.34.57, respectively.

### 5.3.1.2 Restoring FRU Information

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c RestoreFruInfo --file <filename> [--format <file format>]
In-Band	saa -c RestoreFruInfo --file <filename> [--format <file format>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c RestoreFruInfo --file <filename> [--format <file format>] [--remote_saa <remote SAA path>]

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c RestoreFruInfo --file <filename> [--format <file format>] [--individually]
Remote In-Band	saa -I Remote_INB -l <system list file> -c RestoreFruInfo --file <filename> [--format <file format>] [--individually] [--remote_saa <remote saa path>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c RestoreFruInfo
--file dumpedFile --format BINARY
```

#### In-band:

```
[SAA_HOME]# ./saa -c RestoreFruInfo --file dumpedFile
```

#### Remote In-band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c RestoreFruInfo --file dumpedFile --remote_saa /root/saa
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c RestoreFruInfo --
file dumpedFile --format TEXT
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c RestoreFruInfo --
file dumpedFile --format BINARY --individually
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

#### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c RestoreFruInfo --file
dumpedFile --format TEXT --individually
```

```
SList.txt:
192.168.34.56 OS_Username OS_PASSWD
192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

### 5.3.1.3 Changing FRU Information

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChangeFruInfo [--item <item name> --value <assignment value>   --fru_version <FRU version>]
In-Band	saa -c ChangeFruInfo [--item <item name> --value <assignment value>   --fru_version <FRU version>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeFruInfo [--item <item name> --value <assignment value>   --fru_version <FRU version>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeFruInfo
--fru_version 00.01
```

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

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeFruInfo
--item ALL --value "0x01,2,3,2024/01/01 00:00,5,6,7,8,9,10,11,12,13,14"
```

The console output contains the following information.

```
ChangeFruInfo command is completed.
```

```
Chassis Type (CT): 01
```

---

```
Chassis Part Number (CP): 2
Chassis Serial Number (CS): 3
Board mfg. Date/Time (BDT): 2024/01/01 00:00
Board Manufacturer Name (BM): 5
Board Product Name (BPN): 6
Board Serial Number (BS): 7
Board Part Number (BP): 8
Product Manufacturer (PM): 9
Product Name (PN): 10
Product Part/Model Number (PPM): 11
Product Version (PV): 12
Product Serial Number (PS): 13
Product Asset Tag (PAT): 14
```

### **In-Band:**

```
[SAA_HOME]# ./saa -c ChangeFruInfo --fru_version 00.01
```

```
[SAA_HOME]# ./saa -c ChangeFruInfo --item CT --value 0x01
```

### **The console output contains the following information.**

```
ChangeFruInfo command is completed.

Chassis Type (CT): 01
Chassis Part Number (CP):
Chassis Serial Number (CS):
Board mfg. Date/Time (BDT): 2021/08/30 18:01
Board Manufacturer Name (BM): Supermicro
Board Product Name (BPN):
Board Serial Number (BS): WM218S011157
Board Part Number (BP):
Product Manufacturer (PM):
Product Name (PN):
Product Part/Model Number (PPM):
Product Version (PV):
Product Serial Number (PS):
Product Asset Tag (PAT):
```

### **Multiple systems OOB:**

```
[SAA_HOME]# $./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeFruInfo --
item CT --value 0x01
```

```
SList.txt:
192.168.34.56
```

### 5.3.2. Getting System Summary Firmware Image Information

Use the “GetSystemInfo” command to retrieve comprehensive firmware image information from the managed system. This command provides a system-wide summary, encompassing firmware details of components, including System, LAN, BMC, BIOS, CPLD, SCP and Redfish version, if supported.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSystemInfo
In-Band	saa [-l Redfish_HI -u <username> -p <password>] -c GetSystemInfo
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetSystemInfo

Example:

**In - Band :**

```
[SAA_HOME]# ./saa -c GetSystemInfo
```

**The console output contains the following information.**

```
Managed system.....localhost
 IPv4.....10.168.24.116
 BMC MAC address.....3A:EC:EF:CE:41:3B
 Firmware revision.....00.23.37
 Firmware build time.....2021/06/28
 BIOS version.....1.1
 BIOS build time.....06/21/2021
 CPLD version.....F0.09.46
 IPv6.....FE80:0000:0000:0000:AEEC:FFFF:FECE:413B/64
 System LAN1 MAC address...3A:EC:EF:CE:40:0F
 System LAN2 MAC address...3A:EC:EF:CE:40:A5
```

**In-Band Redfish Host Interface:**

---

```
[SAA_HOME]# ./saa -c GetSystemInfo -I Redfish_HI -u ADMIN -p ADMIN
```

**The console output contains the following information.**

```
Managed system.....169.254.4.254
 IPv4.....10.168.24.116
 BMC MAC address.....3A:EC:EF:CE:41:3B
 Firmware revision.....00.23.37
 Firmware build time.....2021/06/28
 BIOS version.....1.1
 BIOS build time.....06/21/2021
 CPLD version.....F0.09.46
 IPv6.....FE80:0000:0000:0000:AEEC:FFFF:FECE:413B/64
 System LAN1 MAC address.....3A:EC:EF:CE:40:0F
 System LAN2 MAC address.....3A:EC:EF:CE:40:A5
 Redfish version.....1.8.0
 Supermicro Redfish version..RF1.11-00.00
```

**OOB:**

```
[SAA_HOME]# $./saa -c GetSystemInfo -i 10.168.29.116 -p ADMIN -u ADMIN
```

**The console output contains the following information.**

```
Managed system.....10.168.29.116
 IPv4.....10.168.29.116
 BMC MAC address.....3A:EC:EF:CE:41:3B
 Firmware revision.....00.23.37
 Firmware build time.....2021/06/28
 BIOS version.....1.1
 BIOS build time.....06/21/2021
 CPLD version.....F0.09.46
 IPv6.....FE80:0000:0000:0000:AEEC:FFFF:FECE:413B/64
 System LAN1 MAC address.....3A:EC:EF:CE:40:0F
 System LAN2 MAC address.....3A:EC:EF:CE:40:A5
 Redfish version.....1.8.0
 Supermicro Redfish version..RF1.11-00.00
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetSystemInfo
```

```
SList.txt:
 192.168.34.56
```



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.

### 5.3.3. Getting System Settings

Use the “GetSystemCfg” command to execute SAA 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 accessed.
- 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 5.7.16 Profile Update.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSystemCfg --file <SystemCfg.xml> [--overwrite] [--download] [--file_id]
In-band	saa -c GetSystemCfg --file <SystemCfg.xml> [--overwrite] [--download] [--file_id]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetSystemCfg --file <SystemCfg.xml> [--overwrite] [--download] [--file_id]

Example:

**OOB:**

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

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

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

#### Multiple OOB:

```
[SAA_HOME]# ./saa -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.

### 5.3.4. Updating the System Settings

1. Follow the steps in 5.3.3 Getting System Settings.
2. Edit the configurable element values in the system configuration file SystemCfg.xml. See the steps in 5.4.4 Updating BIOS Settings Based on the Current BIOS Settings and 5.5.4 Updating BMC Settings.
3. Use the command ChangeSystemCfg with the updated SystemCfg.xml file to run SAA to update the system configuration.

Single System	
OOB	saa -i <BMC IP or host name> -u <username> -p <password> -c ChangeSystemCfg --file <SystemCfg.xml> [--reboot [--post_complete]] saa -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]]

In-band	saa -c ChangeSystemCfg --file <SystemCfg.xml> [--reboot]
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeSystemCfg --file <SystemCfg.xml> [--reboot [--post_complete]] -c ChangeSystemCfg [--update Apply Deploy --dev_id <Device ID> --file_id <file ID> --reboot]   [--upload --file SystemCfg.xml]

Example:

#### OOB:

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

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
ChangeSystemCfg --upload --file SystemCfg.xml
```

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

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

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeSystemCfg --
file SystemCfg.xml
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeSystemCfg --
file SystemCfg.xml --individually
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeSystemCfg --
upload --file SystemCfg.xml
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeSystemCfg --
update Apply --dev_id A1_1,B11_2,A10 --file_id 2 --reboot
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -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, SAA 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.



**Notes:**

- For more details, please refer to 5.4.4 Updating BIOS Settings Based on the Current BIOS Settings and 5.5.4 Updating BMC Settings.
- The connection might be lost if the LAN configuration is changed.
- To update a profile, please refer to 5.7.11 Managing the 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 immediately update the existing Blade system.

---

### 5.3.5 Getting Fan Mode

---

Use the “GetFanMode” command to retrieve the Fan Configuration of the managed system. This command provides the current fan mode and all available fan modes supported by the system.

All Supported fanmode are as below:

Mode	Type
0	Standard
1	Full
2	Optimal
3	PUE2 Optimal
4	Heavy IO
5	PUE3 Optimal
6	Liquid Cooling
7	Smart Cooling

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetFanMode
In-band	saa -c GetFanMode
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetFanMode

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetFanMode
```

---

The console output contains the following information.

```
Current FanMode is "Optimal".
All Available Fan Mode are:
Mode: Type
0: Standard
1: Full
2: Optimal
4: Heavy IO
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetFanMode
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### 5.3.6. Setting the Fan Mode

Use the "SetFanMode" command to set the fan mode for the target system. Afterwards, use the "GetFanMode" command to check if the desired mode has been set successfully.

Single Systems	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SetFanMode --fanmode <fan type>
In-band	saa -c SetFanMode --fanmode <fan type>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SetFanMode >

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetFanMode --fanmode 0
```

---

The console output contains the following information.

```
Fan mode is changed to Standard
All Available Fan Modes are:
Mode: Type
0: Standard
1: Full
2: Optimal
4: Heavy IO
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetFanMode --
fanmode 0
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### 5.3.7 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: 0 = GetStatus 1 = On 2 = Off

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c LocateServerUid --action <action>
In-Band	saa -c LocateServerUid --action <actuib>
Multiple Systems	

OOB	<code>saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c LocateServerUid --action &lt;action&gt;</code>
-----	-------------------------------------------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -c LocateServerUid --action GetStatus
```

The console output contains the following information.

```
Managed system.....localhost
UID status.....Off
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c LocateServerUid --
action 3
```

```
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.

## 5.3.8 Obtaining a summary of Firmware Inventory information



Use the “GetFirmwareInventoryInfo” command to retrieve comprehensive Firmware Inventory information from the managed system. This command provides a system-wide summary.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetFirmwareInventoryInfo [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetFirmwareInventoryInfo [--json_view]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetFirmwareInventoryInfo [--json_view]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetFirmwareInventoryInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
 BMC.....00.23.80
 BMC Backup.....Not Present
 BMC Golden.....00.23.69
 BMC Staging.....00.23.80
 BIOS.....BIOS Date: 11/29/2023 Ver 1.8
 BIOS Backup.....Not Present
 BIOS Golden.....BIOS Date: 07/12/2022 Ver 1.4
 BIOS Staging.....BIOS Date: 11/29/2023 Ver 1.8
 CPLD Motherboard.....F0.09.46
 BIOS ME.....4.4.4.603
```

**In-Band Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
GetFirmwareInventoryInfo
```

---

The console output contains the following information.

```
Managed system.....169.254.3.254
 BMC.....00.23.80
 BMC Backup.....Not Present
 BMC Golden.....00.23.69
 BMC Staging.....00.23.80
 BIOS.....BIOS Date: 11/29/2023 Ver 1.8
 BIOS Backup.....Not Present
 BIOS Golden.....BIOS Date: 07/12/2022 Ver 1.4
 BIOS Staging.....BIOS Date: 11/29/2023 Ver 1.8
 CPLD Motherboard.....F0.09.46
 BIOS ME.....4.4.4.603
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetFirmwareInventoryInfo
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```



**Note:** If the execution “GetFirmwareInventoryInfo” command with the “--json\_view” option to show the Firmware Inventory information results in JSON format.

---

## 5.3.9 Clearing CMOS

Use the “ClearCMOS” command to clear CMOS and reset all BIOS settings to their default values.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ClearCMOS --ac_cycle
In-Band	saa -I Redfish_HI -u <username> -p <password> -c ClearCMOS -- ac_cycle

Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c ClearCMOS --ac_cycle

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c ClearCMOS --ac_cycle
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c ClearCMOS --ac_cycle
```

**The console output contains the following information.**

```
Status: Start to clear CMOS...Done

Proceeding to AC cycle the managed system.
.....Done

Warning: Please wait for BMC to connect for around 3 minutes. Do not remove AC
power before the action is completed.

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

#### Multiple systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ClearCMOS --ac_cycle
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

**Note:**

Clearing the CMOS will initiate an AC power cycle. The BMC will reset, and the system will reboot.

## 5.4. BIOS Management

### 5.4.1. 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).

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c GetBiosInfo [--showall] [--extract_measurement]</code>
In-Band	<code>saa [-I Redfish_HI -u &lt;username&gt; -p &lt;password&gt;] -c GetBiosInfo [--file &lt;filename&gt; [--file_only]] [--showall] [--extract_measurement]</code>
Remote In-Band	<code>saa {-I Remote_INB   -I Remote_RHI -u &lt;username&gt; -p &lt;password&gt;} -oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c GetBiosInfo [--file &lt;filename&gt; [--file_only]] [--showall] [--extract_measurement] [--remote_saa &lt;remote SAA path&gt;]</code>
Multiple Systems	
OOB	<code>saa -I &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c GetBiosInfo [--file &lt;filename&gt;] [--showall]</code>
Remote In-Band	<code>saa {-I Remote_INB   -I Remote_RHI} -I &lt;system list file&gt; -c GetBiosInfo [--file &lt;filename&gt;] [--showall] [--remote_saa &lt;remote SAA path&gt;]</code>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBiosInfo --file Supermicro_BIOS_signed.bin
```

---

**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.bin
 Board ID.....0988
 BIOS build date.....2018/5/7
 FW image.....Signed
 Signed Key.....SecureFlash
```

**In-Band :**

```
[SAA_HOME]# ./saa -c GetBiosInfo --file Supermicro_BIOS_signed.bin --
file_only
```

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

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

```
[SAA_HOME]# ./saa -c GetBiosInfo --file Supermicro_BIOS.bin --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.bin
 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
```

```
[SAA_HOME]# ./saa -c GetBiosInfo --file Supermicro_BIOS.bin --file_only -
-extract_measurement
```

**The console output contains the following information.**

```
Local BIOS image file.....Supermicro_BIOS.bin
Board ID.....1B6A
BIOS build date.....2022/05/27
FW image.....Signed
Signed Key.....RoT
Measurement.....FB0DC09383104F49834E2E903F46F365259CB598
6D97F0F3D9DB5945E0D0DFD59F8511F6857E915B41A1B9A30071EF5D99018144033DCC80464B951E
555402B
```

#### **Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c GetBiosInfo --remote_saa /root/saa
```

#### **Remote In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.57 -
--ou root --op 111111 -c GetBiosInfo --remote_saa /root/saa
```

**The console output contains the following information.**

---

```
Start Remote In-Band execution on 192.168.34.57:
```

```
=====
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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/saa.log' from
'/root/saa_remote_inband/2022-11-03_17-37-49/saa.log' on 192.168.34.57.
```

### Multiple systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBiosInfo --file
Supermicro_BIOS.bin
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetBiosInfo --file
Supermicro_BIOS.bin
```

```
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.

---

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(U)	RoT is NOT signed by Super Micro Computer, Inc. but by an unknown authority.
(Not shown)	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.

## 5.4.2. Updating the BIOS Firmware Image

Use the “UpdateBios” command with the BIOS firmware image Supermicro\_BIOS.bin or bios\_image.tar for OpenBMC to run SAA to update the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateBios --file <filename> [options...]
In-Band	saa [-l <IP or host name> -u <username> -p <password>] -c UpdateBios --file <filename> [options...]
Remote In-Band	saa {-l Remote_INB   -l Remote_RHI -u <username> -p <password>} -oi <OS IP address> --ou <OS username> --op <OS password> -c



	UpdateBios --file <filename> [--remote_saa <remote SAA path>] [options...]
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateBios --file <filename> [options...]
Remote In-Band	saa {-l Remote_INB   -l Remote_RHI} -l <system list file> -c UpdateBios --file <filename> [--remote_saa <remote SAA 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.
--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.
--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.

-- restore_optimized_default	Restores the BIOS configurations to optimized default settings.
---------------------------------	-----------------------------------------------------------------



#### Notes:

- Before performing the OOB UpdateBios command, it is recommended to shut down the managed system first.
- When performing an in-band UpdateBios command, SAA 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 SAA 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 X13SAx series, X12SAE and X12SCA-(5)F.
- 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, SAA 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.
  - 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 GRUB2 loader version is not the latest, 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 firmware files for BIOS firmware updates. Please refer to the Appendix L. Creating a Firmware Updating Tar File for OpenBMC for creating a tar file firmware image.

---

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBios --file Supermicro_BIOS.bin --reboot
```

**In-Band:**

```
[SAA_HOME]# ./saa -c UpdateBios --file Supermicro_BIOS.bin --reboot
```

**In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateBios --file Supermicro_BIOS.bin --reboot
```

**Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c UpdateBios --file Supermicro_BIOS.bin --reboot --remote_saa /root/saa
```

**Remote In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 --ou root --op 111111 -c UpdateBios --file Supermicro_BIOS.bin --reboot --remote_saa /root/saa
```

**Multiple System OoB:**

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateBios --file
Supermicro_BIOS.bin
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c UpdateBios --file
Supermicro_BIOS.bin
```

```
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.



#### 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) for X12 3rd Generation Intel® Xeon® Scalable processors with Intel® C620 Series Chipsets. 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. SAA prevents the BMC from being updated with unauthorized firmware.

---

### 5.4.3. Getting Current BIOS Settings

Use the “`GetCurrentBiosCfg`” command to execute SAA 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.
- The current BIOS settings will be generated as an XML file, which contains extended ASCII characters. Please use ISO 8859-1 encoding to view the BIOS configuration XML file.
- SAA supports text-based user interface (TUI). For details, refer to 4.9 TUI.
- SAA 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 is not supported for Remote In-band usage.

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c GetCurrentBiosCfg [--file &lt;USER_SETUP.file&gt; [--overwrite]] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--tui [--compact]]</code>
In-Band	<code>saa -c GetCurrentBiosCfg [--file &lt;USER_SETUP.file&gt; [--overwrite]] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--tui [--compact]]</code>
Remote In-Band	<code>saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c GetCurrentBiosCfg [--file &lt;USER_SETUP.file&gt; [--overwrite]] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--remote_saa &lt;remote SAA path&gt;]</code>
Multiple Systems	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c GetCurrentBiosCfg [--file &lt;USER_SETUP.file&gt; [--overwrite]] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;]</code>
Remote In-Band	<code>saa -I Remote_INB -l &lt;system list file&gt; -c GetCurrentBiosCfg [--file &lt;USER_SETUP.file&gt; [--overwrite]] [--current_password &lt;current</code>

---

	password>   --cur_pw_file <current password file path>] [--remote_saa <remote SAA path>]
--	------------------------------------------------------------------------------------------

Example:

**OOB:**

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

**In-Band:**

```
[SAA_HOME]# ./saa -c GetCurrentBiosCfg --file USER_SETUP.file --overwrite
```

**Remote In-Band:**

```
[SAA_HOME]# ./saa -l Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
GetCurrentBiosCfg --file USER_SETUP.file --overwrite --remote_saa /root/saa
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetCurrentBiosCfg --file
USER_SETUP.file
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

**Multiple Remote In-Band:**

```
[SAA_HOME]# ./saa -l 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.

#### 5.4.4. Updating BIOS Settings Based on the Current BIOS Settings

1. Follow the steps in 5.4.3 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 4.7.1 BIOS Settings XML File Format.
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 SAA 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.
- 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 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.

- The same boot device may be presented with slightly varied boot strings. BIOS/SAA 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 SAA 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.
- A BIOS configuration tagged with "<LicenseRequirement>" requires the SFT-DCMS-SINGLE node product key to change the BIOS setting. Please refer to Appendix B Management Interface and License Requirements.
- Use the --individually option to update each managed system with the corresponding configuration file for multiple systems.

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c ChangeBiosCfg --file &lt;USER_SETUP.file&gt; [--save_as_user_default] [-- current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot [--post_complete]]  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c ChangeBiosCfg --save_as_user_default [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot [-- post_complete]]</pre>
In-Band	<pre>saa -c ChangeBiosCfg --file &lt;USER_SETUP.file&gt; [-- save_as_user_default] [--current_password &lt;current password&gt;   -- cur_pw_file &lt;current password file path&gt;] [--reboot]  saa -c ChangeBiosCfg --save_as_user_default [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [-- reboot]</pre>

Remote In-Band	<p>saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c ChangeBiosCfg --file &lt;USER_SETUP.file&gt; [--save_as_user_default] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot] [--remote_saa &lt;remote SAA path&gt;]</p> <p>saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c ChangeBiosCfg --save_as_user_default [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot] [--remote_saa &lt;remote SAA path&gt;]</p>
<b>Multiple Systems</b>	
OOB	<p>saa -I &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c ChangeBiosCfg --file &lt;USER_SETUP.file&gt; [--save_as_user_default] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot [--post_complete]] [--individually]</p> <p>saa -I &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c ChangeBiosCfg --save_as_user_default [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot [--post_complete]]</p>
Remote In-Band	<p>saa -I Remote_INB -I &lt;system list file&gt; -c ChangeBiosCfg --file &lt;USER_SETUP.file&gt; [--save_as_user_default] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot] [--individually] [--remote_saa &lt;remote SAA path&gt;]</p> <p>saa -I Remote_INB -I &lt;system list file&gt; -c ChangeBiosCfg --save_as_user_default [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot] [--remote_saa &lt;remote SAA path&gt;]</p>

Example:

#### OOB:

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

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeBiosCfg --file USER_SETUP.file --save_as_user_default --reboot
```

#### In-Band:

---

```
[SAA_HOME]# ./saa -c ChangeBiosCfg --file USER_SETUP.file --reboot
[SAA_HOME]# ./saa -c ChangeBiosCfg --save_as_user_default --reboot
```

#### **Remote In-Band:**

```
[SAA_HOME]# ./saa -l Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c
ChangeBiosCfg --file USER_SETUP.file --reboot --remote_saa /root/saa
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeBiosCfg --file
USER_SETUP.file --reboot
[SAA_HOME]# ./saa -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 Remote In-Band:**

```
[SAA_HOME]# ./saa -l 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, SAA 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.

### **5.4.5. Getting Factory BIOS Settings**

Use the “GetDefaultBiosCfg” command to have SAA get the default factory BIOS settings from the managed system and save it in the USER\_SETUP.file file.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetDefaultBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--current_password <current password>   --cur_pw_file <current password file path>]
In-Band	saa -c GetDefaultBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--current_password <current password>   --cur_pw_file <current password file path>]
Remote In-Band	saa -l Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetDefaultBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--current_password <current password>   --cur_pw_file <current password file path>] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetDefaultBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--current_password <current password>   --cur_pw_file <current password file path>]
Remote In-Band	saa -l Remote_INB -l <system list file> -c GetDefaultBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--current_password <current password>   --cur_pw_file <current password file path>] [--remote_saa <remote SAA path>]

Example:

**OOB:**

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

**In-Band:**

```
[SAA_HOME]# ./saa -c GetDefaultBiosCfg --file USER_SETUP.file --overwrite
```

**Remote In-Band:**

---

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111-c
GetDefaultBiosCfg --file USER_SETUP.file --overwrite --remote_saa /root/saa
```

#### **Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -I SList.txt -u ADMIN -p PASSWORD -c GetDefaultBiosCfg --file
USER_SETUP.file
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

#### **Multiple Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB -I 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.

### **5.4.6. Updating BIOS Settings Based on the Factory Settings**

1. Follow the steps in 5.4.5 Getting Factory BIOS Settings.
2. Follow steps 2 to 4 in 5.4.4 Updating BIOS Settings Based on the Current BIOS Settings.

### **5.4.7. Loading Factory BIOS Settings**

Use the “LoadDefaultBiosCfg” command to have SAA 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.

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c LoadDefaultBiosCfg [--optimized_default] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [-- reboot [--post_complete]]  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c LoadDefaultBiosCfg --show</pre>
In-Band	<pre>saa -c LoadDefaultBiosCfg [--optimized_default] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [-- reboot]  saa -c LoadDefaultBiosCfg --show</pre>
Remote In-Band	<pre>saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c LoadDefaultBiosCfg [--optimized_default] [-- current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--reboot] [--remote_saa &lt;remote SAA path&gt;]  saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c LoadDefaultBiosCfg --show</pre>
Multiple Systems	
OOB	<pre>saa -I &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c LoadDefaultBiosCfg [--optimized_default] [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [-- reboot [--post_complete]]  saa -I &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c LoadDefaultBiosCfg --show</pre>
Remote In-Band	<pre>saa -I Remote_INB -I &lt;system list file&gt; -c LoadDefaultBiosCfg [-- optimized_default] [--current_password &lt;current password&gt;   -- cur_pw_file &lt;current password file path&gt;] [--reboot] [--remote_saa &lt;remote SAA path&gt;]  saa -I Remote_INB -I &lt;system list file&gt; -c LoadDefaultBiosCfg --show</pre>

---

Example:

**OOB:**

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

**In-Band:**

```
[SAA_HOME]# ./saa -c LoadDefaultBiosCfg --show
```

**The console output contains the following information.**

```
Managed system.....localhost
 BIOS default.....Optimized Default
```

**Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c LoadDefaultBiosCfg --reboot --remote_saa /root/saa
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -I SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBiosCfg --optimized_default --reboot
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

**Multiple Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB -I 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
```

**Notes:**

- If you don't use the `--optimized_default` option, the managed system will be restored to its current default setting, which may be the user-selected default or the performance-optimized default setting.
- For platforms that do not support the `--optimized_default` option, the current default setting is the performance-optimized setting.

### 5.4.8. Getting DMI Information

Use the “GetDmiInfo” command to execute SAA 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. SAA will only show supported items.

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c GetDmiInfo [--file &lt;DMI.txt&gt; [--overwrite]]</code>
In-Band	<code>saa [-I Redfish_HI -u &lt;username&gt; -p &lt;password&gt;] -c GetDmiInfo [--file &lt;DMI.txt&gt; [--overwrite]]</code>
Remote In-Band	<code>saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c GetDmiInfo [--file &lt;DMI.txt&gt; [--overwrite]] [--remote_saa &lt;remote SAA path&gt;]</code>
Multiple Systems	
OOB	<code>saa -I &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c GetDmiInfo [--file &lt;DMI.txt&gt; [--overwrite]]</code>
Remote In-Band	<code>saa -I Remote_INB -I &lt;system list file&gt; -c GetDmiInfo [--file &lt;DMI.txt&gt;]</code>



---

	<code>[--overwrite]] [--remote_saa &lt;remote SAA path&gt;]</code>
--	--------------------------------------------------------------------

Example:

**OOB:**

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

**In-Band:**

```
[SAA_HOME]# ./saa -c GetDmiInfo --file DMI.txt --overwrite
```

**Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c GetDmiInfo --file DMI.txt --overwrite --remote_saa /root/saa
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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:**

```
[SAA_HOME]# ./saa -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.

### 5.4.9. 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 5.2.8 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 4.4 DMI Information Text File Format.
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 5.2.8 Getting DMI Information.

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c EditDmiInfo --file &lt;DMI.txt&gt; --item_type &lt;Item Type&gt; --item_name &lt;Item Name&gt;   --shn &lt;Item Short Name&gt;} {--value &lt;Item Value&gt;   --default}</code>
In-Band	<code>saa -c EditDmiInfo --file &lt;DMI.txt&gt; --item_type &lt;Item Type&gt; --item_name &lt;Item Name&gt;   --shn &lt;Item Short Name&gt;} {--value &lt;Item</code>

	Value>   --default}
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c EditDmiInfo [--file <DMI.txt> --item_type <Item Type> --item_name <Item Name>   --shn <Item Short Name>} [--value <Item Value>   --default} [--remote_saa <remote SAA path>]
<b>Multiple Systems</b>	
OOB	saa -I <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}
Remote In-Band	saa -I Remote_INB -I <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_saa <remote SAA path>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --item_type "System" --item_name "Version" --value "1.02"
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --shn SYVS --value "1.02"
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c EditDmiInfo --file
DMI.txt --shn SYVS --default
```

#### In-Band:

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

#### Remote In-Band:

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

#### Multiple Systems OOB:

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c EditDmiInfo --file DMI.txt -
-item_type "System" --item_name "Version" --value "1.01"
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c EditDmiInfo --file DMI.txt -
-shn SYVS --value "1.01"
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -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

## 5.4.10. Updating DMI Information

1. Follow the steps in 5.2.9 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 SAA 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.

- Use the --individually option to update each managed system with the corresponding configuration file for multiple systems.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChangeDmiInfo [--file <DMI.txt>] [--reboot [--post_complete]]
In-Band	saa -c ChangeDmiInfo [--file <DMI.txt>] [--reboot]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c ChangeDmiInfo [--file <DMI.txt>] [--reboot] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c ChangeDmiInfo [--file <DMI.txt>] [--reboot [--post_complete]] [--individually]
Remote In-Band	saa -I Remote_INB -I <system list file> -c ChangeDmiInfo [--file <DMI.txt>] [--reboot] [--individually] [--remote_saa <remote SAA path>]

Example:

#### OOB:

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

#### In-Band:

```
[SAA_HOME]# ./saa -c ChangeDmiInfo --file DMI.txt --reboot
```

#### Remote In-Band:

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

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeDmiInfo --file
DMI.txt --reboot
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -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, SAA 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.

## 5.4.11. Setting Up a BIOS Administrator Password

Use the "SetBiosPassword" command to execute SAA to update the BIOS Administrator password.

Single System	
OOB	saa -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 [--post_complete]]
In-Band	saa -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	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS 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_saa <remote SAA path>]
<b>Multiple Systems</b>	
OOB	saa -I <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 [--post_complete]]
Remote In-Band	saa -I Remote_INB -I <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_saa <remote SAA path>]

For Multiple Systems OOB usage:

The managed systems should be enumerated row by row in the system list file. For the “SetBiosPassword” command, 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.

For Multiple Systems Remote In-Band usage:

Two formats are supported for Multiple Remote In-Band as follow:

**Format 1:** OS\_IP\_or\_HostName OS\_Username OS\_Password New\_BIOS\_Password  
Current\_BIOS\_Password

**Format 2:** OS\_IP\_or\_HostName OS\_Username OS\_PrivateKey  
OS\_Privatekey\_Password New\_BIOS\_Password Current\_BIOS\_Password

SAA 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:

**O0B:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBiosPassword --
new_password 123456 --confirm_password 123456 --current_password 654321 --
reboot
```

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

**In-Band:**



---

```
[SAA_HOME]# ./saa -c SetBiosPassword --new_password 123456 --confirm_password 123456 --reboot
```

```
[SAA_HOME]# ./saa -c SetBiosPassword --pw_file passwd.txt --cur_file cur_passwd.txt --reboot
```

```
passwd.txt:
 BiosPassword
cur_passwd.txt:
 BiosPassword
```

### Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c SetBiosPassword --new_password 123456 --confirm_password 123456 --reboot --remote_saa /root/saa
```

```
[SAA_HOME]# ./saa -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_saa /root/saa
```

```
passwd.txt:
 BiosPassword
cur_passwd.txt:
 BiosPassword
```

```
SList.txt:
 192.168.34.56 new_ pwd_11 current_pwd_1
 192.168.34.57 ADMIN1 PASSWORD1 new_pwd_22 current_pwd_2
```

To specify new password and current password corresponding to each system, you can use the example below with system list file SList.txt.

```
[SAA_HOME]# ./saa -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_1 1
192.168.34.57	ADMIN1	PASSWORD1	new_pwd_22	current_pwd_2 2

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.

```
[SAA_HOME]# ./saa -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

### 5.4.12. Erasing the BIOS OA Key

Use the “EraseOAKey” command to have SAA 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.

Single System	
In-Band	saa -c EraseOAKey [--reboot]

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c EraseOAKey [--reboot] [--remote_saa <remote SAA path>]
----------------	----------------------------------------------------------------------------------------------------------------------------------------

Example:

**In-Band :**

```
[SAA_HOME]# ./saa -c EraseOAKey --reboot
```

**Remote In-Band :**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c EraseOAKey --reboot --remote_saa /root/saa
```

### 5.4.13. Managing 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.



**Note:** The Seamless Update feature is only supported on X13 RoT platforms or later.

#### • Seamless Update Feature in UpdateBios Command

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateBios --file <CAPSULE_FILE.bin> [--staged update] [--reboot [--post_complete]]
In-Band	saa [-I <IP or host name> -u <username> -p <password>] -c UpdateBios --file <CAPSULE_FILE.bin> [--staged update] [--reboot]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateBios --file <CAPSULE_FILE.bin> [--remote_saa <remote SAA path>] [--staged update] [--reboot]

Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateBios --file <CAPSULE_FILE.bin> [--staged update] [--reboot [--post_complete]]
Remote In-Band	saa -l Remote_RHI -l <system list file> -c UpdateBios --file <CAPSULE_FILE.bin> [--remote_saa <remote SAA path>] [--staged update] [--reboot]

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 an 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 they 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, they 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.

Example:

#### OOB:

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

#### In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateBios --file CAPSULE_FILE.bin --reboot
```

#### Remote In-Band through Redfish Host Interface:

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

### Multiple System OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -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**

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBiosInfo --file <CAPSULE_FILE.bin> [--showall]
In-Band	saa [-l <IP or host name> -u <username> -p <password>] -c GetBiosInfo --file <CAPSULE_FILE.bin> [--showall]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetBiosInfo --file <CAPSULE_FILE.bin> [--remote_saa <remote SAA path>] [--showall]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c

	GetBiosInfo --file <CAPSULE_FILE.bin> [--showall]
Remote In-Band	saa -I Remote_RHI -I <system list file> -c GetBiosInfo --file <CAPSULE_FILE.bin> [--remote_saa <remote SAA path>] [--showall]

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 the 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 the managed system.

Example:

#### **OOB:**

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

#### **In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetBiosInfo --file CAPSULE_FILE.bin
```

#### **Remote In-Band through Redfish Host Interface:**

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

---

### Multiple System OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -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
```

## 5.4.14. Getting SCP Firmware Image Information

Use the “GetScpInfo” command to get the System Control Processor (SCP) firmware image information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetScpInfo
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetScpInfo
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetScpInfo

Example:

#### OOB:

```
[SAA_HOME]# ./saa -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 :**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetScpInfo
```

The console output contains the following information.

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

**Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -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.

---

### 5.4.15. Updating the SCP Firmware Image

Use the “UpdateScp” command with SCP firmware image scp\_image.tar to run SAA to update the managed system.



**Notes:**

- BMC only accepts the tar firmware file for SCP firmware updates. To create a .tar firmware image, refer to Appendix 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, SAA 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 4.3.3 Redfish Host Interface.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateScp --file <filename> --reboot [--post_complete]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c UpdateScp --file <filename> --reboot
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateScp --file <filename> --reboot [--post_complete]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -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.
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateScp --file
scp_image.tar
```

```
SList.txt:
 192.168.34.56
```

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.

### 5.4.16. 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetFixedBootCfg [--file <filename>] [--overwrite] --redfish
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetFixedBootCfg [--file <filename>] [--overwrite] --redfish
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c GetFixedBootCfg --file <USER_SETUP.file> [--overwrite] --redfish

Example:

**OOB:**

```
./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetFixedBootCfg --redfish
--file FixedBootCfg.xml --overwrite
```

**In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c GetFixedBootCfg --
redfish --file FixedBootCfg.xml --overwrite
```

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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
```

### 5.4.17. Updating the Fixed Boot Setting

1. Follow the steps in 5.4.16. 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 4.7.8. Fixed Boot Configuration XML File Format.
3. Use the “ChangeFixedBootCfg” command with the updated file USER\_SETUP.file to run SAA to update the Fixed Boot configuration.



#### 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 UEFI Network 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.
  - The change will take effect after the managed system is rebooted.
  - Use the --individually option to update each managed system with the corresponding configuration file.
-

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChangeFixedBootCfg --file <USER_SETUP.file> [--reboot [--post_complete]] --redfish
In-Band	saa -I Redfish_HI -u <username> -p <password> -c ChangeFixedBootCfg --file <USER_SETUP.file> [--reboot] --redfish
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeFixedBootCfg --file <USER_SETUP.file> [--reboot [--post_complete]] [--individually] --redfish

Example:

#### OOB:

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

#### In-Band:

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

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l Slist.txt -u ADMIN -p PASSWORD -c ChangeFixedBootCfg
--file USER_SETUP.file --reboot --redfish
```

```
[SAA_HOME]# ./saa -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, SAA 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.

### 5.4.18. Getting Boot Option

Use the "GetBootOption" command to get the boot option from the target system. GetBootOption can get NextBootOnly , BypassPassword and Device Type.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBootOption
In-Band	saa -c GetBootOption
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetBootOption

Example:

#### OOB:

```
./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBootOption
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GetBootOption
```

The console output contains the following information.

```
NextBootOnly.....Enable
BypassPassword.....Disable
DeviceType.....0:No Override
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBootOption
```

```
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.

### 5.4.19. Setting Boot Option

Use the "SetBootOption" command to set the boot options for the target system. The SetBootOption command can configure the NextBootOnly, BypassPassword, and Device Type settings. If you do not use the "--next\_boot\_only" and "--bypass\_password" options, the default value will be "Disable." After executing the SetBootOption command, no power operations will be performed. However, if you use the "- -action" option, power operations will be carried out.

Command Options	Descriptions
--action	Sets action to: 0 = up 1 = down 2 = cycle 3 = reset 4 = softshutdown 5 = reboot

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SetBootOption --device_type <Device Type ID> [--next_boot_only <Enable   Disable>] [--bypass_password <Enable   Disable>] [--action <action>] [--post_complete]
In-Band	saa -c SetBootOption --device_type <Device Type ID> [--next_boot_only <Enable   Disable>] [--bypass_password <Enable   Disable>] [--action <action>]
Multiple Systems	

OOB	saa -l < system list file > [-u <username> -p <password>] -c SetBootOption --device_type <Device Type ID> [--next_boot_only <Enable   Disable>] [--bypass_password <Enable   Disable>] [--action <action> [--post_complete]]
-----	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBootOption -- device_type 0 --next_boot_only Enable --bypass_password Enable -- action 5
```

#### In-Band:

```
[SAA_HOME]# ./saa -c SetBootOption -c SetBootOption --device_type 0 -- next_boot_only Enable --bypass_password Enable --action 5
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBootOption -- device_type 0 --next_boot_only Enable --bypass_password Enable --action 5
```

```
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.

## 5.4.20. Booting into an ISO Image from an HTTP Server

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SetHttpBoot [--current_password <current password>   --cur_pw_file



	<pre>&lt;current password file path&gt;] [--boot_lan &lt;boot lan port&gt;] [--boot_name &lt;boot description&gt;] --image_url &lt;URL&gt; [--reboot [--post_complete]] [--file &lt;file name&gt;]</pre> <pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetHttpBoot --boot_clean [--reboot [--post_complete]]</pre>
In-Band	<pre>saa -c SetHttpBoot [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--boot_lan &lt;boot lan port&gt;] [--boot_name &lt;boot description&gt;] --image_url &lt;URL&gt; [--reboot] [--file &lt;file name&gt;]</pre> <pre>saa -c SetHttpBoot --boot_clean [--reboot]</pre>
<b>Multiple Systems</b>	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetHttpBoot [--current_password &lt;current password&gt;   --cur_pw_file &lt;current password file path&gt;] [--boot_lan &lt;boot lan port&gt;] [--boot_name &lt;boot description&gt;] --image_url &lt;URL&gt; [--reboot [--post_complete]] [--file &lt;file name&gt;]</pre> <pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetHttpBoot --boot_clean [--reboot [--post_complete]]</pre>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetHttpBoot --boot_clean --reboot
```

#### In-Band:

```
[SAA_HOME]# ./saa -c SetHttpBoot --boot_name bootDescription --image_url http://192.168.12.78/iso/efishell.iso --reboot
```

---

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -c SetHttpBoot --boot_clean --reboot
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetHttpBoot --
boot_name bootDescription --image_url
http://192.168.12.78/iso/efishell.iso --reboot
```

```
[SAA_HOME]# ./saa -l 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
```

```
[SAA_HOME]# ./saa -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 --boot\_clean option 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 startup.nsh file.
-

---

## 5.4.21. Getting BIOS POST Codes

Use the “GetBiosPostCode” command to get BIOS POST codes.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBiosPostCode
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetBiosPostCode
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetBiosPostCode [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBiosPostCode
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetBiosPostCode [--remote_saa <remote SAA path>]

Example:

### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBiosPostCode
```

### In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetBiosPostCode
```

### Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p ADMIN --oi 192.168.34.56 --ou root --op 111111 -c GetBiosPostCode --remote_saa /root/saa
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBiosPostCode
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetBiosPostCode
```

```
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 console output for a single system contains the following information.

```
SuperServer Automation Assistant 1.0.0 (2023/08/23) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.56:
=====
SuperServer Automation Assistant 1.0.0 (2023/08/23) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

The BIOS POST code : 9e
=====

Getting file 'remote_inband/2023-08-23_15-04-37_10.184.21.173/saa.log' from
'/root/saa_remote_inband/2023-08-23_15-04-38/saa.log' on 192.168.34.56.

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

## 5.5. BMC Management

### 5.5.1. 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.

#### Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBmcInfo [--file <filename> [--extract_measurement]] [--showall]
In-Band	saa [-l <IP or host name> -u <username> -p <password>] -c GetBmcInfo [--file <filename> [--extract_measurement]] [--showall]
Remote In-Band	saa -l Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> [--remote_saa <remote SAA path>] -c GetBmcInfo [--file <filename> [--extract_measurement]] [--showall]
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetBmcInfo [--file <filename> [--extract_measurement]] [--showall]
Remote In-Band	saa -l Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c GetBmcInfo [--file <filename> [--extract_measurement]] [--showall]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBmcInfo --file Supermicro_BMC.bin
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GetBmcInfo --file Supermicro_BMC.bin
```

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

```
Managed system.....localhost
 BMC type.....X12_RoT_ATEN_AST2500
 BMC version.....00.23.37
 BMC ext. version....01 00 00 (P)
 BMC build date.....2021/06/28

Local BMC image file..../home/user/BMC_X13AST2600-nonRoT-
0501MS_20230807_01.01.13_STDsp.bin
 BMC UFFN.....BMC_X13AST2600-0501MS_20230807_01.01.13_STDsp.bin
 BMC type.....X13_ATEN_AST2600_1_1
 BMC version.....01.01.13
```

---

```
BMC build date.....2023/08/07
FW image.....Signed
Signed Key.....NonRoT
```

```
[SAA_HOME]# ./saa -c GetBmcInfo --file Supermicro_ROT_BMC.bin --file_only
```

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

```
Local BMC image file.....Supermicro_ROT_BMC.bin
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
```

```
[SAA_HOME]# ./saa -c GetBmcInfo --file Supermicro_ROT_BMC.bin --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.....CE772709B937E6F256A09B9CEDFB9F7F4195B19143543964FD00C900BD73F1F3
6743724B34392B06D4D1D5542CFA0619C32AF960B93A3973A4F2101762A8698D
```

```
[SAA_HOME]# ./saa -c GetBmcInfo --file Supermicro ROT BMC.bin --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:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c GetBmcInfo --file Supermicro_BMC.bin
```

**The console output for a single system contains the following information when the local BMC image is non-RoT signed.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.57:
=====
SuperServer Automation Assistant 1.0.0_alpha (2023/08/18) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Managed system.....localhost
 BMC type.....X12_RoT_ATEN_AST2500
 BMC version.....00.23.37
 BMC ext. version.....01 00 00 (P)
 BMC build date.....2021/06/28

Local BMC image file...../home/user/BMC_X13AST2600-nonRoT-
0501MS_20230807_01.01.13_STDsp.bin
 BMC UFFN.....BMC_X13AST2600-0501MS_20230807_01.01.13_STDsp.bin
 BMC type.....X13_ATEN_AST2600_1_1
 BMC version.....01.01.13
 BMC build date.....2023/08/07
 FW image.....Signed
 Signed Key.....NonRoT
=====

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

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

### Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.57 -
--ou root --op 111111 -c GetBmcInfo --file Supermicro_BMC.bin
```

### Multiple Systems 00B:

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBmcInfo --file
Supermicro_BMC.bin
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetBmcInfo --file
Supermicro_BMC.bin
```

```
SList.txt:
192.168.34.56 OS_Username OS_PASSWD
192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetBmcInfo --file
Supermicro_BMC.bin
```

```
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.

FW image signed of a local BMC image displays the following information:

Type	Descriptions
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.
Signed(C)	The key is NOT signed by Super Micro Computer, Inc., but by the



	specified certificate.
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.

## 5.5.2. Updating the BMC Firmware Image

Use the “UpdateBmc” command with BMC firmware image Supermicro\_BMC.bin or bmc\_image.tar for OpenBMC to run SAA 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 --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 --skip\_unknown option is designed to skip all invalid tables and settings in the latest BMC configuration in the managed system.
- For details on updating BMC firmware with preservation of BMC settings, please refer to 5.5.2.1 Updating BMC Firmware with BMC Settings Preservation.

Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl]
In-Band	saa [-I <IP or host name> -u <username> -p <password>] -c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI -u <username> -p <password>} -oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl] [--remote_saa <remote SAA path>]
<b>Multiple Systems</b>	
OOB	saa -I < system list file > [-u <username> -p <password>] -c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI} -I <system list file> -c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl] [--remote_saa <remote SAA path>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBmc --file Supermicro_BMC.bin
```

#### In-Band:

```
[SAA_HOME]# ./saa -c UpdateBmc --file Supermicro_BMC.bin
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateBmc --file Supermicro_BMC.bin
```

#### Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c UpdateBmc --file Supermicro_BMC.bin
```

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateBmc --file
Supermicro_BMC.bin
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c UpdateBmc --file
Supermicro_BMC.bin
```

```
SList.txt:
192.168.34.56 OS_Username OS_PASSWD
192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c UpdateBmc --file
Supermicro_BMC.bin
```

```
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.

### 5.5.2.1 Updating BMC Firmware with Preservation of BMC Settings

To update BMC firmware with preservation of settings and avoid setting backward compatibility, follow these steps.

1. Update the BMC to the latest firmware while preserving the BMC configuration. By default, when the UpdateBmc command is executed without the --overwrite\_cfg option, the BMC configurations are preserved.

Command Mode	Command Usage
--------------	---------------



Command Mode	Command Usage
Inband	<code>./saa -c GetBmcCfg [--file bmccfg.xml [--overwrite]]</code>
OOB	<code>./saa -i &lt;BMC IP&gt; -u &lt;username&gt; -p &lt;password&gt; -c GetBmcCfg [--file bmccfg.xml [--overwrite]]</code>

The console output contains the following information.

```
SuperServer Automation Assistant 1.0.0 (2024/05/02) (x86_64)
Copyright(C) 2024 Super Micro Computer, Inc. All rights reserved.

.....
File "bmccfg.xml" is created
```

### 3. Modify the BMC configuration file.

For example, change the <LanInterface> field from "Failover" to "Dedicated" within the <LAN> table of the BMC configuration file.

```
<LAN Action="Change">
 <!--Supported Action:None/Change-->
 <Information>
 <!--Information for LAN properties-->
 <MacAddress>7C:C2:55:19:85:2B</MacAddress>
 <SpeedMbps>1000</SpeedMbps>
 <Duplex>Full Duplex</Duplex>
 </Information>
 <Configuration>
 <!--Configuration for LAN properties-->
 <IPProtocolStatus>Dual</IPProtocolStatus>
 <!--IPv4/IPv6/Dual-->
 <!--The value shall indicate which IP protocol can be accessed.-->
 <LanInterface>Dedicated</LanInterface>
 <!--Dedicated/Shared/Failover-->
 <!--Changing this setting may cause the LAN to be unavailable.-->
 <Link>Auto Negotiation</Link>
 <!--Auto Negotiation/100M Half Duplex/100M Full Duplex/1G Full Duplex-->
 <!--Link can only be updated if LanInterface is Dedicated.-->
 <!--Link will be empty if LanInterface is Shared.-->
 <!--Will be skipped if empty.-->
 <HostName></HostName>
 <!--BMC host name-->
 <!--string value; length limit = 63 characters-->
```

### 4. Change the BMC configuration with the modified configuration file.

Command Mode	Command Usage
Inband	<code>./saa -c ChangeBmcCfg [--file bmccfg.xml [--overwrite]]</code>
OOB	<code>./saa -i &lt;BMC IP&gt; -u &lt;username&gt; -p &lt;password&gt; -c ChangeBmcCfg [--file bmccfg.xml]</code>

The console output contains the following information.

---

```
SuperServer Automation Assistant 1.0.0 (2024/05/02) (x86_64)
Copyright(C) 2024 Super Micro Computer, Inc. All rights reserved.
```

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

```
Status: Start updating the BMC configuration for 192.168.34.56
```

```
*****WARNING*****
*
```

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

```

*
```

```
.....
```

```
Status: The BMC configuration is updated for 192.168.34.56
```

### 5.5.3. Getting BMC Settings

Use the “GetBmcCfg” command to have SAA 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.
- SAA 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.
- SAA supports pure Redfish LAN tables in the BMC configuration. For more details, please refer to 4.5.1 Pure Redfish LAN Table in BMC Configuration.

---

Single System
---------------

OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--dump] [--overwrite]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--dump] [--overwrite]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI -u <username> -p <password>} -oi <OS IP address> --ou <OS username> --op <OS password> -c GetBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--dump] [--overwrite] [-remote_saa <remote SAA path>]
<b>Multiple Systems</b>	
OOB	saa -I <system list file> [-u <username> -p <password>] -c GetBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--dump] [--overwrite]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI} -I <system list file> -c GetBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--dump] [--overwrite] [-remote_saa <remote SAA path>]

Example:

#### OOB:

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

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

#### In-Band:

```
[SAA_HOME]# ./saa -c GetBmcCfg --file BMCCfg.xml --overwrite
```

```
[SAA_HOME]# ./saa -c GetBmcCfg --file BMCCfg.bin --dump --overwrite
```

#### Remote In-Band:

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

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

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBmcCfg --file BMCCfg.xml --overwrite
```

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetBmcCfg --file BMCCfg.xml --overwrite
```

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetBmcCfg --file BMCCfg.xml --overwrite
```

```
[SAA_HOME]# ./saa -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 setting 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.

### 5.5.3.1 Generating BMC Settings Format Based on Sample File

Configurations in BMC firmware can have various XML formats across different versions. To get the configuration of an older BMC firmware from the managed system, use the GetBmcCfg command and specify the table format with the "--sample\_file" option.

The "--sample\_file" option only supports for X13/H13 or later platforms.



#### Notes:

- The tables/elements received may vary between two managed systems. Only the supported tables/elements for the managed system will be received.
- For in-band, Redfish host interface and OOB usages, note that the file formats for getting BMC settings may be different. Ensure that the sample file source aligns with the current command execution mode.
- When you use the --sample\_file option, do not remove table fields in the sample file. If the table version in the sample file cannot be recognized, the table will not be generated.

---

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBmcCfg --file <BMCCfg.xml> [--overwrite] [--sample_file<config_format.xml>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetBmcCfg --file <BMCCfg.xml> [--overwrite] [--sample_file<config_format.xml>]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI -u <username> -p <password>} - -oi <OS IP address> --ou <OS username> --op <OS password> -c GetBmcCfg --file <BMCCfg.xml> [--overwrite] [--sample_file<config_format.xml>]

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBmcCfg --file <BMCCfg.xml> [--overwrite] [--sample_file<config_format.xml>]
Remote In-Band	saa {-l Remote_INB   -l Remote_RHI} -l <system list file> -c GetBmcCfg --file <BMCCfg.xml> [--overwrite] [--sample_file<config_format.xml>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBmcCfg --file BMCCfg.xml --overwrite --sample_file config_format.xml
```

#### Inband:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBmcCfg --file BMCCfg.xml --overwrite --sample_file config_format.xml
```

#### Remote In-band:

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

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBmcCfg --file BMCCfg.xml --overwrite --sample_file config_format.xml
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBmcCfg --file BMCCfg.xml --overwrite --sample_file config_format.xml
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## 5.5.4. Updating BMC Settings

1. Select one managed system as the golden sample for current BMC settings. (For multiple systems)
2. Follow the steps in 5.5.3 Getting BMC settings.
3. Edit the configurable element values in the BMC configuration text file BMCCfg.xml to the desired values as illustrated in 4.5 BMC Configuration XML File Format.
4. Skip unchanged tables in the text file by setting the 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 updated BMCCfg.xml file to run SAA to update the BMC configuration or restore it with the BMCCfg.bin file by the "--restore" option.

Single System	
OOB	saa -i <P or host name> -u <username> -p <password> -c ChangeBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--restore] [--skip_unknown]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c ChangeBmcCfg -file <BMCCfg.xml   BMCCfg.bin> [--restore] [--skip_unknown]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI -u <username> -p <password>} -oi <OS IP address> --ou <OS username> --op <OS password> -c ChangeBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--restore] [--skip_unknown] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c ChangeBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--restore] [--skip_unknown] [--individually]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI} -I <system list file> -c ChangeBmcCfg --file <BMCCfg.xml   BMCCfg.bin> [--restore] [--skip_unknown] [--individually] [--remote_saa <remote SAA path>]

Example:

**OOB:**

---

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

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

#### **In-Band:**

```
[SAA_HOME]# ./saa -c ChangeBmcCfg --file BMCCfg.xml
```

```
[SAA_HOME]# ./saa -c ChangeBmcCfg --file BMCCfg.bin --restore
```

#### **Remote In-Band:**

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

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

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcCfg --
file BMCCfg.xml
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcCfg --
file BMCCfg.bin --restore
```

```
[SAA_HOME]# ./saa -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:**

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ChangeBmcCfg --file
BMCCfg.xml --individually
```

---

```
[SAA_HOME]# ./saa -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 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, SAA 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.

**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.
- SAA supports pure Redfish LAN tables in the BMC configuration. For more details, please refer to 4.5.1 Pure Redfish LAN Table in BMC Configuration.

---

### 5.5.5 Installing BMC Certification

To enhance security, SAA 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)

### 5.5.6. Setting Up a BMC User Password

Use the “SetBmcPassword” command to have SAA update the BMC user password.

Single System	
OOB	saa -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>]]
In-Band	saa -c SetBmcPassword [--user_id <user ID>] [--new_password <new password> --confirm_password <confirm password>]   [--pw_file <password file path>]]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SetBmcPassword [--user_id <user ID>] [--new_password <new password> --confirm_password <confirm password>]   [--pw_file <password file path>]] [--remote_saa <remote SAA path>]
Multiple Systems	

---

OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetBmcPassword [--user_id &lt;user ID&gt;] {[--new_password &lt;new password&gt; --confirm_password &lt;confirm password&gt;]   [--pw_file &lt;password file path&gt;]}</code>
Remote In-Band	<code>saa -l Remote_INB -l &lt; system list file&gt; -c SetBmcPassword [--user_id &lt;user ID&gt;] {[--new_password &lt;new password&gt; --confirm_password &lt;confirm password&gt;]   [--pw_file &lt;password file path&gt;]} [--remote_saa &lt;remote SAA path&gt;]</code>

For Multiple Systems OOB usage:

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.

For Multiple Systems Remote In-Band usage:

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:

**OOB:**

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

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

**In-Band:**

```
[SAA_HOME]# ./saa -c SetBmcPassword --new_password 12345678 --
confirm_password 12345678
```

```
[SAA_HOME]# ./saa -c SetBmcPassword --user_id 3 --pw_file passwd.txt
```

```
passwd.txt:
BmcPasswordString
```

**Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c SetBmcPassword --user_id 3 --pw_file passwd.txt
```

```
passwd.txt:
BmcPasswordString
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcPassword
```

```
SList.txt:
192.168.34.56 12345678
192.168.34.57 ADMIN1 PASSWORD1 87654321
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcPassword --
new_password 12345678 --confirm_password 12345678
```



```
[SAA_HOME]# ./saa -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
```

## 5.5.7 Getting the BMC KCS Privilege Level

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetKcsPriv
In-Band	saa -c GetKcsPriv
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetKcsPriv [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetKcsPriv
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetKcsPriv [--remote_saa <remote SAA path>]

Example:

### OOB:

```
./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetKcsPriv
```

### In-Band:

```
[SAA_HOME]# ./saa -c GetKcsPriv
```

### Remote In-Band:

```
[SAA_HOME]# ./saa -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)
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetKcsPriv
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

#### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -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
```

## 5.5.8 Setting the BMC KCS Privilege Level

Use the “SetKcsPriv” command to have SAA set the BMC KCS privilege level.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SetKcsPriv {--priv_level <KCS privilege level>}
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SetKcsPriv {--priv_level <KCS privilege level>}

Example:

---

## OOB:

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

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

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetKcsPriv --priv_level 'Call Back'
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetKcsPriv --priv_level 1'
```

```
SList.txt:
192.168.34.56
192.168.34.57
```



### Notes:

- SAA 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 numeric ID or a name.
- 

## 5.5.9. Loading Factory BMC Settings

Supermicro has implemented a new security feature for the BMC firmware stack. 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 SAA 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.

Action Option	Reset Network	Reset User Cfg	Reset FRU	Reset Password to
-- preserve_use r_cfg	N	N	N	Preserved
-- clear_user_cf g with -- load_default_ password	N	Y	N	ADMIN
-- clear_user_cf g with -- load_unique_ password	N	Y	N	Unique Password
-- clear_user_cf g with -- load_unique_ password and -- load_default_l an	Y	Y	N	Unique Password
-- clear_user_cf g with -- load_unique_ password, -- load_default_l an and -- load_default_f ru	Y	Y	Y	Unique Password

Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c LoadDefaultBmcCfg [--preserve_user_cfg   --clear_user_cfg [--load_default_password   --load_unique_password [--load_default_lan [--load_default_fru]]]] [--bmc_boot_check [--reboot [--post_complete]]] [--redfish]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c LoadDefaultBmcCfg [--preserve_user_cfg   --clear_user_cfg [--load_default_password   --load_unique_password [--load_default_lan [--load_default_fru]]]] [--bmc_boot_check [--reboot]] [--redfish]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI -u <username> -p <password>} -oi <OS IP address> --ou <OS username> --op <OS password> -c LoadDefaultBmcCfg [--preserve_user_cfg   --clear_user_cfg [--load_default_password   --load_unique_password [--load_default_lan [--load_default_fru]]]] [--bmc_boot_check [--reboot]] [--redfish] [--remote_saa <remote SAA path>]
<b>Multiple Systems</b>	
OOB	saa -I <system list file> [-u <username> -p <password>] -c LoadDefaultBmcCfg [--preserve_user_cfg   --clear_user_cfg [--load_default_password   --load_unique_password [--load_default_lan [--load_default_fru]]]] [--bmc_boot_check [--reboot [--post_complete]]] [--redfish]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI} -I <system list file> -c LoadDefaultBmcCfg [--preserve_user_cfg   --clear_user_cfg [--load_default_password   --load_unique_password [--load_default_lan [--load_default_fru]]]] [--bmc_boot_check [--reboot]] [--redfish] [--remote_saa <remote SAA path>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p ADMIN -c LoadDefaultBmcCfg
--preserve_user_cfg --bmc_boot_check --reboot --post_complete
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
LoadDefaultBmcCfg --clear_user_cfg --load_unique_password
```

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

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
LoadDefaultBmcCfg --clear_user_cfg --load_unique_password --
load_default_lan --load_default_fru
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c LoadDefaultBmcCfg --preserve_user_cfg
```

```
[SAA_HOME]# ./saa -c LoadDefaultBmcCfg --clear_user_cfg --
load_unique_password
```

```
[SAA_HOME]# ./saa -c LoadDefaultBmcCfg --clear_user_cfg --
load_default_password
```

```
[SAA_HOME]# ./saa -c LoadDefaultBmcCfg --clear_user_cfg --
load_unique_password --load_default_lan --load_default_fru
```

#### **Remote In-Band**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c LoadDefaultBmcCfg --preserve_user_cfg
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg
--preserve_user_cfg
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg
--clear_user_cfg --load_unique_password
```

```
[SAA_HOME]# ./saa -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 Remote In-Band:**

```
[SAA_HOME]# ./saa -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
```



**Notes:**

- The --load\_unique\_password option only works on systems installed with a unique BMC password.
- The --bmc\_boot\_check option is not compatible with In-Band pure Redfish usage on X14/B14 systems. This is because resetting the BMC configuration disables the Redfish host interface by default on these systems.

### 5.5.10. Setting the BMC Reset Counter

Use the “TimedBmcReset” command to set the BMC reset counter for the target system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c TimedBmcReset [--delay <BMC reset delay time>   --immediate [--bmc_boot_check]]
In-Band	saa -c TimedBmcReset [--delay <BMC reset delay time>   --immediate [--bmc_boot_check]]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c TimedBmcReset [--delay <BMC reset delay time>   --immediate [--bmc_boot_check]] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c TimedBmcReset [--delay <BMC reset delay time>   --immediate [--bmc_boot_check]]
Remote In-Band	saa -I Remote_INB -I <system list file> -c TimedBmcReset [--delay <BMC reset delay time>   --immediate [--bmc_boot_check]] [--remote_saa <remote SAA path>]

Example:

---

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TimedBmcReset
--delay 1
```

**The console output contains the following information.**

```
The BMC will be reset after 1 minute.
```

```
[SAA_HOME]# ./saa -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.
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TimedBmcReset
--immediate --bmc_boot_check
```

**The console output contains the following information.**

```
The BMC will be reset immediately.
Please wait a few minutes for the BMC to restart.
.....
.....
Done.
```

**In-Band:**

```
[SAA_HOME]# ./saa -c TimedBmcReset --delay 1
```

```
[SAA_HOME]# ./saa -c TimedBmcReset --immediate --bmc_boot_check
```

**Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c TimedBmcReset --delay 1 --remote_saa /root/saa
```



---

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c TimedBmcReset --immediate --bmc_boot_check --remote_saa /root/saa
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TimedBmcReset --
delay 1
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TimedBmcReset --
immediate --bmc_boot_check
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c TimedBmcReset --delay 1
```

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c TimedBmcReset --immediate
--bmc_boot_check
```

```
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, 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:

The --delay option is only supported on X11/H11 and earlier platforms.

---

## 5.5.11. Getting BMC LAN Settings

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

**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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBmcLANCfg [--file <BMCLANCfg.xml> [--overwrite]]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetBmcLANCfg [--file <BMCLANCfg.xml> [--overwrite]]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI -u <username> -p <password>} -oi <OS IP address> --ou <OS username> --op <OS password> -c GetBmcLANCfg [--file <BMCLANCfg.xml> [--overwrite]] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c GetBmcLANCfg [--file <BMCLANCfg.xml> [--overwrite]]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI} -I <system list file> -c GetBmcLANCfg [--file <BMCLANCfg.xml> [--overwrite]] [--remote_saa <remote SAA path>]

Example:

**OOB:**

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

**In-Band:**

```
[SAA_HOME]# ./saa -c GetBmcLANCfg --file BMCLANCfg.xml --overwrite
```

---

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

#### **Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
GetBmcLANCfg --file BMCLANCfg.xml --overwrite
```

#### **Remote In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.57 -
-ou root --op 111111 GetBmcLANCfg --file BMCLANCfg.xml --overwrite
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBmcLANCfg --
file BMCLANCfg.xml --overwrite
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

#### **Multiple Systems Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetBmcLANCfg --file
BMCLANCfg.xml --overwrite
```

```
SList.txt:
192.168.34.56 OS_Username OS_PASSWD
192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetBmcLANCfg --file
BMCLANCfg.xml --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 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.

### 5.5.12. Updating BMC LAN Settings

1. Select one managed system as the golden sample for current BMC LAN settings. (For multiple systems)
2. Follow the steps in 5.5.11 Getting BMC LAN Settings.
3. Edit the configurable element values in the BMC LAN configuration text file BMCLANCfg.xml to the desired values described as those in 4.7.3 BMC LAN Configuration XML File Format.
4. Skip the unchanged tables in the text file by setting the Action attribute to “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 “ChangeBmcLanCfg” command with the updated BMCLANCfg.xml file to run SAA to update the BMC LAN configuration.
7. The IPv4 settings *IPAddr*, *SubNetmask*, *DefaultGateWayAddr* in the *IPv4* table cannot be applied to each managed system. (For multiple systems)
8. Use the --individually option to update each managed system with the corresponding configuration file. (For multiple systems)

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChangeBmcLanCfg --file <BMCLANCfg.xml> [--skip_unknown]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c ChangeBmcLanCfg --file <BMCLANCfg.xml> [--skip_unknown]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI -u <username> -p <password>} -oi <OS IP address> --ou <OS username> --op <OS password> -c ChangeBmcLanCfg --file <BMCLANCfg.xml> [--skip_unknown] [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeBmcLANCfg --file <BMCLANCfg.xml> [--skip_unknown] [--individually]
Remote In-Band	saa {-I Remote_INB   -I Remote_RHI} -l <system list file> -c ChangeBmcLANCfg --file <BMCLANCfg.xml> [--skip_unknown] [--individually] [--remote_saa <remote SAA path>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
ChangeBmcLANCfg --file BMCCfg.xml
```

#### In-Band:

```
[SAA_HOME]# ./saa -c ChangeBmcLANCfg --file BMCLANCfg.xml --overwrite
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c ChangeBmcLANCfg -
-file BMCLANCfg.xml
```

#### Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
GetBmcLANCfg --file BMCLANCfg.xml --overwrite
```

#### Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.57 -
-ou root --op 111111 GetBmcLANCfg --file BMCLANCfg.xml --overwrite
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcLANCfg --
file BMCLANCfg.xml
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeBmcLANCfg --
file BMCLANCfg.xml --individually
```

```
SList.txt:
192.168.34.56
```

---

```
192.168.34.57
```

### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ChangeBmcLANCfg --file
BMCLANCfg.xml
```

```
SList.txt:
192.168.34.56 OS_Username OS_PASSWD
192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c ChangeBmcLANCfg --file
BMCLANCfg.xml --individually
```

```
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, 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, SAA 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.



#### 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.

### 5.5.13. Getting the BMC User List

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBmcUserList
In-Band	saa [-l Redfish_HI -u <username> -p <password>] -c GetBmcUserList
Remote In-Band	saa {-l Remote_INB   -l Remote_RHI -u <username> -p <password>} -oi <OS IP address> --ou <OS username> --op <OS password> -c GetBmcUserList [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBmcUserList
Remote In-Band	saa {-l Remote_INB   -l Remote_RHI} -l <system list file> -c GetBmcUserList [--remote_saa <remote SAA path>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetBmcUserList
```

The console output contains the following information.

```
Maximum number of Users : 16
Count of currently enabled Users : 1
User ID | User Name | Privilege Level | Enabled | Account Types
===== | ===== | ===== | ===== | =====
 2 | ADMIN | Administrator | Yes | Redfish/IPMI
===== | ===== | ===== | ===== | =====
```

---

The BMC user list.

### In-Band:

```
[SAA_HOME]# ./saa -c GetBmcUserList
```

The console output contains the following information.

```
Maximum number of Users : 10
Count of currently enabled Users : 1
User ID | User Name | Privilege Level | Enabled
=====|=====|=====|=====
 2 | ADMIN | Administrator | Yes
=====|=====|=====|=====
```

The BMC user list.

### In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetBmcUserList
```

The console output contains the following information.

```
Maximum number of Users : 16
Count of currently enabled Users : 1
User ID | User Name | Privilege Level | Enabled | Account Types
=====|=====|=====|=====|=====
 2 | ADMIN | Administrator | Yes | Redfish/IPMI
=====|=====|=====|=====|=====
```

The BMC user list.

### Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GetBmcUserList --remote_saa /root/saa
```

### Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p ADMIN --oi 192.168.34.56 --ou
root --op 111111 -c GetBmcUserList --remote_saa /root/saa
```



---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBmcUserList
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetBmcUserList
```

```
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 Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetBmcUserList
```

```
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 console output of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

### 5.5.14. Setting the BMC User List

Use the “SetBmcUserList” command to set the current BMC user list for the target 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 a BMC user's privilege**

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

- **Change a BMC user password**

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

- **Test BMC user login**

Use the “SetBmcUserList” command with the “--action Test” option to verify a BMC user login.

- **Enable the BMC user type**

Use the “SetBmcUserList” command with the “--action EnableType” option to activate a BMC user type.

- **Enable a BMC user**

Use the “SetBmcUserList” command with the “--action EnableAccount” option to activate a BMC user status.

- **Edit the BMC user name**

Use the “SetBmcUserList” command with the “--action EditUserName” option to edit a BMC user name.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SetBmcUserList --action add --user_id <userid> --user_name <username> --user_password <userpassword> --user_privilege

	<pre> &lt;userprivilege&gt; [--user_status &lt;status&gt;] [--manage_account_type &lt;type:status&gt;] [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]]  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList --action &lt;action&gt; --user_id &lt;userid&gt; [--user_name &lt;username&gt;] [--user_password &lt;userpassword&gt;] [--user_privilege &lt;userprivilege&gt;]  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList --action Test --user_name &lt;username&gt; -- user_password &lt;userpassword&gt;  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList --action EnableType --user_id {--account_type &lt;type&gt; --account_type_status &lt;status&gt;   --manage_account_type &lt;type:status&gt;} [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList --action EnableAccount --user_id &lt;userid&gt; -- user_status &lt;status&gt;  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList --action EditUserName --user_id &lt;userid&gt; -- user_name &lt;username&gt; </pre>
In-Band	<pre> saa -c SetBmcUserList --action add --user_id &lt;userid&gt; --user_name &lt;username&gt; --user_password &lt;userpassword&gt; --user_privilege &lt;userprivilege&gt;  saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList -- action add --user_id &lt;userid&gt; --user_name &lt;username&gt; -- user_password &lt;userpassword&gt; --user_privilege &lt;userprivilege&gt; [-- user_status &lt;status&gt;] [--manage_account_type &lt;type:status&gt;] [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]]  saa -c SetBmcUserList --action &lt;action&gt; --user_id &lt;userid&gt; [-- user_name &lt;username&gt;] [--user_password &lt;userpassword&gt;] [-- user_privilege &lt;userprivilege&gt;]  saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList -- action Test --user_name &lt;username&gt; --user_password &lt;userpassword&gt;  saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList -- action EnableType --user_id {--account_type &lt;type&gt; -- account_type_status &lt;status&gt;   --manage_account_type &lt;type:status&gt;} [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]  saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList -- action EnableAccount --user_id &lt;userid&gt; --user_status &lt;status&gt; </pre>

	<pre>saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c SetBmcUserList -- action EditUserName --user_id &lt;userid&gt; --user_name &lt;username&gt;</pre>
Remote In-Band	<pre>saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c SetBmcUserList --action add --user_id &lt;userid&gt; -- user_name &lt;username&gt; --user_password &lt;userpassword&gt; -- user_privilege &lt;userprivilege&gt;</pre> <pre>saa -I Remote_RHI -u &lt;username&gt; -p &lt;password&gt; --oi &lt;OS IP address&gt; --ou &lt;OS username&gt;--op &lt;OS password&gt; -c SetBmcUserList --action add --user_id &lt;userid&gt; --user_name &lt;username&gt; --user_password &lt;userpassword&gt; --user_privilege &lt;userprivilege&gt; [--user_status &lt;status&gt;] [--manage_account_type &lt;type:status&gt; [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]]</pre> <pre>saa -I Remote_INB --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c SetBmcUserList --action &lt;action&gt; --user_id &lt;userid&gt; [--user_name &lt;username&gt;] [--user_password &lt;userpassword&gt;] [--user_privilege &lt;userprivilege&gt;]</pre> <pre>saa -I Remote_RHI -u &lt;username&gt; -p &lt;password&gt; --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c SetBmcUserList --action Test --user_name &lt;username&gt; -- user_password &lt;userpassword&gt;</pre> <pre>saa -I Remote_RHI -u &lt;username&gt; -p &lt;password&gt; --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c SetBmcUserList --action EnableType --user_id {--account_type &lt;type&gt; --account_type_status &lt;status&gt;   --manage_account_type &lt;type:status&gt;} [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]</pre> <pre>saa -I Remote_RHI -u &lt;username&gt; -p &lt;password&gt; --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c SetBmcUserList --action EnableAccount --user_id &lt;userid&gt; -- user_status &lt;status&gt;</pre> <pre>saa -I Remote_RHI -u &lt;username&gt; -p &lt;password&gt; --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; -c SetBmcUserList --action EditUserName --user_id &lt;userid&gt; -- user_name &lt;username&gt;</pre>
<b>Multiple Systems</b>	
OOB	<pre>saa -I &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetBmcUserList --action add --user_id &lt;userid&gt; --user_name &lt;username&gt; --user_password &lt;userpassword&gt; --user_privilege &lt;userprivilege&gt; [--user_status &lt;status&gt;] [--manage_account_type &lt;type:status&gt; [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]]</pre> <pre>saa -I &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetBmcUserList --action &lt;action&gt; --user_id &lt;userid&gt; [--user_name</pre>

	<pre> &lt;username&gt;] [--user_password &lt;userpassword&gt;] [--user_privilege &lt;userprivilege&gt;]  saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetBmcUserList --action Test --user_name &lt;username&gt; -- user_password &lt;userpassword&gt;  saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetBmcUserList --action EnableType --user_id {--account_type &lt;type&gt; --account_type_status &lt;status&gt;   --manage_account_type &lt;type:status&gt;} [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]  saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetBmcUserList --action EnableAccount --user_id &lt;userid&gt; -- user_status &lt;status&gt;  saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetBmcUserList --action EditUserName --user_id &lt;userid&gt; -- user_name &lt;username&gt; </pre>
Remote In-Band	<pre> saa -l Remote_INB -l &lt; system list file&gt; -c SetBmcUserList --action add --user_id &lt;userid&gt; --user_name &lt;username&gt; --user_password &lt;userpassword&gt; --user_privilege &lt;userprivilege&gt; [--remote_saa &lt;remote SAA path&gt;]  saa -l Remote_RHI -l &lt; system list file&gt; -c SetBmcUserList --action add --user_id &lt;userid&gt; --user_name &lt;username&gt; --user_password &lt;userpassword&gt; --user_privilege &lt;userprivilege&gt; [--user_status &lt;status&gt;] [--manage_account_type &lt;type:status&gt;] [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]] [--remote_saa &lt;remote SAA path&gt;]  saa -l Remote_INB -l &lt; system list file&gt; -c SetBmcUserList --action &lt;action&gt; --user_id &lt;userid&gt; [--user_name &lt;username&gt;] [-- user_password &lt;userpassword&gt;] [--user_privilege &lt;userprivilege&gt;] [-- remote_saa &lt;remote SAA path&gt;]  saa -l Remote_RHI -l &lt; system list file&gt; -c SetBmcUserList --action Test --user_name &lt;username&gt; --user_password &lt;userpassword&gt; [-- remote_saa &lt;remote SAA path&gt;]  saa -l Remote_RHI -l &lt; system list file&gt; -c SetBmcUserList --action EnableType --user_id { --account_type &lt;type&gt; --account_type_status &lt;status&gt;   --manage_account_type &lt;type:status&gt;} [--ap &lt;protocol&gt; -- pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;] [--remote_saa &lt;remote SAA path&gt;]  saa -l Remote_RHI -l &lt; system list file&gt; -c SetBmcUserList --action EnableAccount --user_id &lt;userid&gt; --user_status &lt;status&gt; [-- remote_saa &lt;remote SAA path&gt;]  saa -l Remote_RHI -l &lt; system list file&gt; -c SetBmcUserList --action </pre>

---

	EditUserName --user_id <userid> --user_name <username> [--remote_saa <remote SAA path>]
--	-----------------------------------------------------------------------------------------

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action Add --user_id 3 --user_name NAME3 --user_password PASSWORD3 --
user_privilege 3 --user_status Disable --manage_account_type
SNMP:Enable,Redfish:Disable --ap SHA --pp DES --ak AKEY3 --pk PKEY3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action Del --user_id 3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
---action Level --user_id 3 --user_privilege 3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action SetPwd --user_id 3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action Test --user_name NAME3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action EnableType --user_id 3 --account_type SNMP --account_type_status
enable --ap 0 --pp DES --ak KEY --pk KEY
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action EnableAccount --user_id 3 --user_status Disable
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action EditUserName --user_id 3 --user_name NAME4
```

**In-Band:**

```
[SAA_HOME]# ./saa -c SetBmcUserList --action 1 --user_id 3 --user_name
NAME3 --user_password PASSWORD3 --user_privilege 3
```

```
[SAA_HOME]# ./saa -c SetBmcUserList --action 2 --user_id 3
```

---

```
[SAA_HOME]# ./saa -c SetBmcUserList --action 3 --user_id 3 --
user_privilege 3
```

```
[SAA_HOME]# ./saa -c SetBmcUserList --action 4 --user_id 3 --
user_password PASSWORD3
```

### **In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 1 --user_id 3 --user_name NAME3 --user_password PASSWORD3 --
user_privilege 3 --user_status Disable --manage_account_type
SNMP:Enable,Redfish:Disable --ap SHA --pp 1 --ak KEY --pk KEY
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 5 --user_name NAME3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 6 --user_id 3 --account_type SNMP --account_type_status enable --
ap SHA --pp 1 --ak KEY --pk KEY
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 6 --user_id 3 --manage_account_type SNMP:Enable,Redfish:Disable --
ap SHA --pp 1 --ak KEY --pk KEY
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 7 --user_id 3 --user_status Disable
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 8 --user_id 3 --user_name NAME4
```

### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action Add --user_id 3 --user_name NAME3 --user_password PASSWORD3 --
user_privilege 3 --user_status Disable --manage_account_type
SNMP:Enable,Redfish:Disable --ap SHA --pp DES --ak AKEY3 --pk PKEY3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action Del --user_id 3
```

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action Level --user_id 3 --user_privilege 3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action SetPwd --user_id 3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action Test --user_name NAME3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action EnableType --user_id 3 --account_type SNMP --account_type_status
enable --ap 0 --pp DES --ak KEY --pk KEY
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action EnableAccount --user_id 3 --user_status Disable
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action EditUserName --user_id 3 --user_name NAME4
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetBmcUserList --action 1
--user_id 3 --user_name NAME3 --user_password PASSWORD3 --user_privilege
3
```

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetBmcUserList --action 2
--user_id 3
```

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetBmcUserList --action 3
--user_id 3 --user_privilege 3
```

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetBmcUserList --action 4
--user_id 3 --user_password PASSWORD3
```

```
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 Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 1
--user_id 3 --user_name NAME3 --user_password PASSWORD3 --user_privilege
3 --user_status Disable --manage_account_type SNMP:Enable,Redfish:Disable
--ap SHA --pp 1 --ak KEY --pk KEY
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 5
--user_name NAME3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 6
--user_id 3 --account_type SNMP --account_type_status enable --ap SHA --
pp 1 --ak KEY --pk KEY
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 6
--user_id 3 --manage_account_type SNMP:Enable,Redfish:Disable --ap SHA --
pp 1 --ak KEY --pk KEY
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 7
--user_id 3 --user_status Disable
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 8
--user_id 3 --user_name NAME4
```

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 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 "No Access" user privilege is not supported.

- The "--action EnableType" and "--action EnableAccount" are not supported on platforms before X12/H12.

### 5.5.15 Bootstrapping an Account for Redfish Host Interface

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

Single System	
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c BootStrappingAccount --action <CreateAccount   DeleteAccount   CheckAccount> [--user_name <username>]

Example:

#### In-Band :

```
[SAA_HOME]# ./saa -c BootStrappingAccount --action 1
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c BootStrappingAccount
--action 1
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c BootStrappingAccount
--action 3
```

---

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c BootStrappingAccount
--action 2 --user_name 'xxxxxxxxxxxxxxxx'
```

### 5.5.16. Managing a RMCP Service Port

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c RmcpManage --action <GetInfo Enable Disable> [--port <port>]
In-Band	saa -c RmcpManage --action <GetInfo Enable Disable> [--port <port>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c RmcpManage --action <GetInfo Enable Disable> [--port <port>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c RmcpManage --
action Enable --port RMCP:623
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c RmcpManage --
action Enable --port 623
```

#### In-Band:

---

```
[SAA_HOME]# ./saa -c RmcpManage --action Enable --port RMCP:623
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c RmcpManage --
action Enable --port RMCP:623
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### 5.5.17. Getting and Setting the BMC Host Name

Use the “BmcHostName” command to get and set the BMC host name.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BmcHostName --action <action> [--hostname <hostname>]
In-Band	saa -c BmcHostName --action <action> [--hostname <hostname>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c BmcHostName --action <action> [--hostname <hostname>] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcHostName --action <action> [--hostname <hostname>]
Remote In-Band	saa -I Remote_INB -l <system list file> -c BmcHostName --action <action> [--hostname <hostname>] [--remote_saa <remote SAA path>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BmcHostName --
action Get
```

The console output contains the following information.

---

```
Managed system.....192.168.34.56
Host name.....testHostName
```

### **In-Band:**

```
[SAA_HOME]# ./saa -c HostName --action Get
```

```
[SAA_HOME]# ./saa -c HostName --action Set -- BmcHostName testHostName
```

### **Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c BmcHostName --action Get --remote_saa /root/saa
```

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c BmcHostName --action Set --hostname testHostName --remote_saa
/root/saa
```

### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BmcHostName --
action Get
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BmcHostName --
action Set --hostname testHostName
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### **Multiple Systems Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c BmcHostName --action Get
```

```
SList.txt:
192.168.34.56 OS_Username OS_PASSWD
192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
```

## **5.5.18. Getting the BMC Session Information**

---

Use the “GetSessionInfo” command to get BMC session information.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSessionInfo
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetSessionInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSessionInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
 SessionHandler.....01h
 Number of possible active sessions....60
 Number of currently active sessions...1
 User ID.....02h
 Operating Privilege Level.....04h
 Session protocol auxiliary data.....11h
 IP Address of remote console.....C0 A8 00 64 (192.168.0.100)
 Mac Address of remote console.....00 00 00 00 00 00 (00:00:00:00:00:00)
 Port Number.....85 94 (38021)
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetSessionInfo
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

## 5.5.19 Managing the Redfish Host Interface

---

Use the “ManageRHI” command to switch USB connection to the CDC-ECM or RNDIS mode.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ManageRHI --action <GetConnection   SetConnection> [--type <RNDIS   CDC_ECM>]
In-Band	saa -c ManageRHI --action <GetConnection   SetConnection> [--type <RNDIS   CDC_ECM>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ManageRHI --action <GetConnection   SetConnection> [--type <RNDIS   CDC_ECM>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c ManageRHI --action GetConnection
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c ManageRHI --action SetConnection
```

**In-Band:**

```
[SAA_HOME]# ./saa -c ManageRHI --action GetConnection
```

```
[SAA_HOME]# ./saa -c ManageRHI --action SetConnection --type CDC_ECM
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ManageRHI --action GetConnection
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## 5.5.20 BmcWatchDog

Use the BmcWatchDog command to set a timer with the corresponding timer action. Then, execute the reset action to start the timer, and use the info action to retrieve the current timer information.

Option Commands	Descriptions
--action	Sets action to: 0 = Set 1 = Info 2 = Reset

Option Commands	Descriptions
--timer_action	Sets action to: 0 = NoAction 1 = HardReset 2 = PowerDown 3 = PowerCycle

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c BmcWatchDog --action Set --timer_action &lt;BmcWatchDog timer actions&gt; --interval &lt;time interval&gt; --countdown &lt;BmcWatchDog count down&gt;</pre> <pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c BmcWatchDog --action &lt;Info   Reset&gt;</pre>
In-Band	<pre>saa -c BmcWatchDog --action Set --timer_action &lt;BmcWatchDog timer actions&gt; --interval &lt;time interval&gt; --countdown &lt;BmcWatchDog count down&gt;</pre> <pre>saa -c BmcWatchDog --action &lt;Info   Reset&gt;</pre>
Multiple Systems	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c BmcWatchDog --action Set --timer_action &lt;BmcWatchDog timer actions&gt; --interval &lt;time interval&gt; --countdown &lt;BmcWatchDog count down&gt;</pre>



---

<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c BmcWatchDog --action &lt;Info   Reset&gt;</pre>
---------------------------------------------------------------------------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p ADMIN -c BmcWatchDog --
action set --timer_action 1 --interval 10 --countdown 60
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p ADMIN -c BmcWatchDog --
action info
```

**In-Band:**

```
[SAA_HOME]# ./saa -c BmcWatchDog --action set --timer_action 0 --interval
10 --countdown 60
```

```
[SAA_HOME]# ./saa -c BmcWatchDog --action set --timer_action 3 --interval
10 --countdown 60
```

The console output contains the following information.

Item		Value
----		-----
Watchdog Timer Use		SMS/OS (0x04)
Watchdog Timer Is		Stopped
Watchdog Timer Actions		Hard Reset (0x01)
Pre-timeout interval		10 seconds
Timer Expiration Flags		0x10
Initial Countdown		20 sec
Present Countdown		0 sec

**Multiple Systems OOB:**

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p ADMIN -c BmcWatchDog --action
set --timer_action 2 --interval 10 --countdown 60
```

```
[SAA_HOME]# ./saa -l IP_ADDR_RANGE.txt -u ADMIN -p ADMIN -c BmcWatchDog -
-action reset
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

**Notes:**

- With the CountDown option, the value must be set between 0 to 6553.
  - With the Interval option, the value must be set between 0 to 255.
  - Please set the Interval to less than 3 counts.
- 

## 5.5.21 Managing Simple Network Management Protocol

SNMPManage command can manage Simple Network Management Protocol (SNMP) for BMC. The following table summarizes the supported actions in SNMPManage command.

Option	--action
Description	GetStatus = Get BMC SNMP status. On = Set SNMP server on. Off = Set SNMP server off. GetCommunityString = Get community string. SetCommunityString = Set community string.

The following chapters will describe each action in detail.

### 5.5.21.1 Getting BMC Simple Network Management Protocol Status

Use the SNMPManage command with option --action GetStatus to get BMC Simple Network Management Protocol (SNMP) status.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SNMPManage --action GetStatus
In-Band	saa -c SNMPManage --action GetStatus
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SNMPManage --action GetStatus

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SNMPManage --action GetStatus
```

#### In-Band:

```
[SAA_HOME]# ./saa -c SNMPManage --action GetStatus
```

The console output contains the following information.

```

Done
Seq IP MAC Acknowledge
--- -- --- -
1 0.0.0.0 00:00:00:00:00:00 off
2 0.0.0.0 00:00:00:00:00:00 off
3 0.0.0.0 00:00:00:00:00:00 off
4 0.0.0.0 00:00:00:00:00:00 off
5 0.0.0.0 00:00:00:00:00:00 off
6 0.0.0.0 00:00:00:00:00:00 off
7 0.0.0.0 00:00:00:00:00:00 off
8 0.0.0.0 00:00:00:00:00:00 off
9 0.0.0.0 00:00:00:00:00:00 off
10 0.0.0.0 00:00:00:00:00:00 off
11 0.0.0.0 00:00:00:00:00:00 off
12 0.0.0.0 00:00:00:00:00:00 off
13 0.0.0.0 00:00:00:00:00:00 off
14 0.0.0.0 00:00:00:00:00:00 off
15 0.0.0.0 00:00:00:00:00:00 off

```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SNMPManage --
action GetStatus
```

```
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.

### 5.5.21.2 Setting Simple Network Management Protocol Server On

Use the SNMPManage command with option --action On to set Simple Network Management Protocol (SNMP) server on.

Option	Description
--snmp_id	Assigns SNMP index. SNMP index: [1-15]
--snmp_ip	Sets SNMP IP
--snmp_mac	Sets SNMP MAC address

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SNMPManage --action On --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>]
In-Band	saa -c SNMPManage --action On --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SNMPManage --action On --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>]

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SNMPManage --
action On -snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>]
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c SNMPManage --action On -snmp_id <snmp id> --snmp_ip
<snmp ip> [--snmp_mac <snmp mac>]
```

**The console output contains the following information.**

```
Done
Seq IP MAC Acknowledge
--- -- --- -
1 192.168.34.56 12:34:56:78:9A:BC on
2 0.0.0.0 00:00:00:00:00:00 off
3 0.0.0.0 00:00:00:00:00:00 off
4 0.0.0.0 00:00:00:00:00:00 off
5 0.0.0.0 00:00:00:00:00:00 off
6 0.0.0.0 00:00:00:00:00:00 off
7 0.0.0.0 00:00:00:00:00:00 off
8 0.0.0.0 00:00:00:00:00:00 off
9 0.0.0.0 00:00:00:00:00:00 off
10 0.0.0.0 00:00:00:00:00:00 off
11 0.0.0.0 00:00:00:00:00:00 off
12 0.0.0.0 00:00:00:00:00:00 off
13 0.0.0.0 00:00:00:00:00:00 off
14 0.0.0.0 00:00:00:00:00:00 off
15 0.0.0.0 00:00:00:00:00:00 off
```

#### **Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SNMPManage --
action On -snmp_id <snmp id> --snmp_ip <snmp ip> --snmp_mac <snmp mac>
```

```
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.

### **5.5.21.3 Setting Simple Network Management Protocol Server Off**

Use the SNMPManage command with option --action On to set Simple Network Management Protocol (SNMP) server off.

Option	Description
--snmp_id	Assigns SNMP index. SNMP index: [1-15]
--snmp_ip	Sets SNMP IP
--snmp_mac	Sets SNMP MAC address

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SNMPManage --action Off --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>]
In-Band	saa -c SNMPManage --action Off --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SNMPManage --action Off --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SNMPManage --
action Off --snmp_id <snmp id> --snmp_ip <snmp ip> --snmp_mac <snmp mac>
```

#### In-Band:

```
[SAA_HOME]# ./saa -c SNMPManage --action Off --snmp_id <snmp id> --snmp_ip
<snmp ip> --snmp_mac <snmp mac>
```

The console output contains the following information.

```
Done
Seq IP MAC Acknowledge
```

```

--- -- --- -----
1 192.168.34.56 12:34:56:78:9A:BC on
2 0.0.0.0 00:00:00:00:00:00 off
3 0.0.0.0 00:00:00:00:00:00 off
4 0.0.0.0 00:00:00:00:00:00 off
5 0.0.0.0 00:00:00:00:00:00 off
6 0.0.0.0 00:00:00:00:00:00 off
7 0.0.0.0 00:00:00:00:00:00 off
8 0.0.0.0 00:00:00:00:00:00 off
9 0.0.0.0 00:00:00:00:00:00 off
10 0.0.0.0 00:00:00:00:00:00 off
11 0.0.0.0 00:00:00:00:00:00 off
12 0.0.0.0 00:00:00:00:00:00 off
13 0.0.0.0 00:00:00:00:00:00 off
14 0.0.0.0 00:00:00:00:00:00 off
15 0.0.0.0 00:00:00:00:00:00 off

```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SNMPManage --
action Off -snmp_id <snmp id> --snmp_ip <snmp ip> --snmp_mac <snmp mac>
```

```

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.

#### 5.5.21.4 Getting BMC Simple Network Management Protocol Community String

Use the SNMPManage command with option --action GetCommunityString to get Simple Network Management Protocol (SNMP) community string.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SNMPManage --action GetCommunityString
In-Band	saa -c SNMPManage --action GetCommunityString
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c

	SNMPManage --action GetCommunityString
--	----------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD --c SNMPManage --
action GetCommunityString
```

#### In-Band:

```
[SAA_HOME]# ./saa -c SNMPManage --action GetCommunityString
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SNMPManage --
action GetCommunityString
```

```
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.

### 5.5.21.5 Setting BMC Simple Network Management Protocol Community String

Use the SNMPManage command with option --action SetCommunityString to set Simple Network Management Protocol (SNMP) community string.

Option	Description
--community string	Sets community string

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SNMPManage --action SetCommunityString --community_string <community_string>



In-Band	saa -c SNMPManage --action SetCommunityString --community_string <community_string>
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SNMPManage --action SetCommunityString --community_string <community_string>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SNMPManage --
action SetCommunityString --community_string <community_string>
```

#### In-Band:

```
[SAA_HOME]# ./saa -c SNMPManage --action SetCommunityString --
community_string <community_string>
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SNMPManage --
action SetCommunityString --community_string <community_string>
```

```
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.

## 5.6. System Event Log

### 5.6.1. Getting System Event Log

Use the “GetEventLog” command to execute SAA 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetEventLog [--info   --mfg] [--raw_data] [--no_banner] [--year   --month   --day] [--format CSV] [--redfish] [--file <EventLog.txt> [--overwrite]]
In-Band	saa [-l Redfish_HI -u <username> -p <password>] -c GetEventLog [--info   --mfg] [--raw_data] [--no_banner] [--year   --month   --day] [--format CSV] [--file <EventLog.txt> [--overwrite]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetEventLog [--info   --mfg] [--raw_data] [--no_banner] [--year   --month   --day] [--format CSV] [--redfish] [--file <EventLog.txt> [--overwrite]]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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
```

---

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetEventLog --info
```

**The console output contains the following information.**

```
Total Entries: 32
SEL Version: 1.5
Free Space: 65535 bytes
Recent Entry Added: 2023/08/23 00:56:11
Recent Entry Erased: 2023/08/19 18:41:24
Number of alloc units: 512
Alloc unit size: 20 bytes
Number of free alloc unit: 480
Largest free blk: 480
Max record size: 20
Get/Set SEL Time: 2023/08/28 05:37:12
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetEventLog --format csv --file EventLog
```

**The console output contains the following information.**

```
Event ID, Created Time, Sensor Type, Severity, Message,
1, 2023-11-04T20:27:08Z, OEM, OK, [LAN-0005] Dedicated LAN Link Up,
2, 2023-11-04T20:32:51Z, OEM, OK, [LAN-0003] System NIC (1) Link Up,
3, 2023-11-04T20:32:51Z, OEM, Warning, [LAN-0004] System NIC (2) Link Down,
4, 2023-11-04T20:37:54Z, OEM, OK, [LAN-0003] System NIC (1) Link Up,
5, 2023-11-04T20:59:12Z, OEM, OK, [LAN-0003] System NIC (1) Link Up,
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetEventLog --month 1
```

---

## The console output contains the following information.

```
Event:1 Time:10/25/2023 09:02:05 Type:System
Assertion: #0FF (System)| Event = Dedicated LAN Link Up

Event:2 Time:10/25/2023 09:02:16 Type:Physical Security (Chassis Intrusion)
Assertion: Chassis Intru| Event = undefined

Event:3 Time:10/25/2023 09:02:22 Type:Temperature
Assertion: M2_SSD2 Temp| Event = Upper Critical - going high
Reading = 71.00 C, Threshold = 70.00 C

Event:4 Time:10/25/2023 09:08:00 Type:System
Assertion: #0FF (System)| Event = Dedicated LAN Link Up

Event:5 Time:10/25/2023 09:08:10 Type:Physical Security (Chassis Intrusion)
Assertion: Chassis Intru| Event = undefined
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetEventLog --
mfg
```

```
1| 01/31/2023 01:15:55 | Assertion: PS1 Status | Type: Power Supply
| Event = Presence detected

2| 02/04/2023 15:56:06 | Assertion: VDimmABCD | Type: Voltage
| Event = Upper Critical - going high
| Reading = 2.04 V, Threshold = 1.37 V

3| 02/04/2023 15:56:06 | Assertion: VDimmABCD | Type: Voltage
| Event = Upper Non-recoverable - going high
| Reading = 2.04 V, Threshold = 1.40 V

4| 02/04/2023 15:56:15 | Deassertion: VDimmABCD | Type: Voltage
| Event = Upper Non-recoverable - going high
| Reading = 1.23 V, Threshold = 1.40 V

5| 02/04/2023 15:56:15 | Deassertion: VDimmABCD | Type: Voltage
| Event = Upper Critical - going high
| Reading = 1.23 V, Threshold = 1.37 V
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetEventLog --
redfish
```

Event ID	Created Time	Sensor Type	Severity	Message
-----	-----	-----	-----	-----
1   LAN Link Up - Assert	2024-03-30T19:14:05Z	OEM	OK	[LAN-0005] Dedicated
2   (1) Link Up - Assert	2024-03-30T19:16:39Z	OEM	OK	[LAN-0003] System NIC
3   (1) Link Up - Assert	2024-03-30T19:34:57Z	OEM	OK	[LAN-0003] System NIC
4   (2) Link Down - Assert	2024-03-30T19:34:57Z	OEM	Warning	[LAN-0004] System NIC
5   LAN Link Up - Assert	2024-03-30T19:40:44Z	OEM	OK	[LAN-0005] Dedicated

#### In-band:

```
[SAA_HOME]# ./saa -c GetEventLog --file EventLog.txt --no_banner --
overwrite
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetEventLog --
raw_data --file EventLog.txt
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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 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.

## 5.6.2. Clearing the System Event Log

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

### Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c ClearEventLog [--current_password <current password>   --cur_pw_file <current password file path>] [--reboot [--post_complete]] [--clear_bmc_eventlog] [--clear_bios_eventlog]
In-Band	saa -c ClearEventLog [--current_password <current password>   --cur_pw_file <current password file path>] [--reboot] [--clear_bmc_eventlog] [--clear_bios_eventlog]
<b>Multiple Systems</b>	
OOB	saa -l <system list file> -u <username> -p <password> -c ClearEventLog [--current_password <current password>   --cur_pw_file <current password file path>] [--reboot [--post_complete]] [--clear_bmc_eventlog] [--clear_bios_eventlog]

Example:

**OOB:**

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

**In-Band:**

```
[SAA_HOME]# ./saa -c ClearEventLog --reboot
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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.

### 5.6.3. Getting System Maintenance Event Log

Use the “GetMaintenEventLog” command to have SAA 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetMaintenEventLog [--st <start time> --et <end time>] [--count <log count>] [--file < MaintenEventLog.txt> [--overwrite]]
In-Band	saa -c GetMaintenEventLog [--st <start time> --et <end time>] [--count <log count>] [--file < MaintenEventLog.txt> [--overwrite]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetMaintenEventLog [--st <start time> --et <end time>] [--count <log count>] [--file < MaintenEventLog.txt> [--overwrite]]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetMaintenEventLog --file MaintenEventLog.txt --overwrite
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetMaintenEventLog --count 5 --file MaintenEventLog.txt --overwrite
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetMaintenEventLog --st 20200601 --et 20200602 --file MaintenEventLog.txt
--overwrite
```

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

#### In-Band:

---

```
[SAA_HOME]# ./saa -c GetMaintenEventLog --file MaintenEventLog.txt --
overwrite
```

```
[SAA_HOME]# ./saa -c GetMaintenEventLog --count 5 --file
MaintenEventLog.txt --overwrite
```

```
[SAA_HOME]# ./saa -c GetMaintenEventLog --st 20200601 --et 20200602 --
file MaintenEventLog.txt --overwrite
```

```
[SAA_HOME]# ./saa -c GetMaintenEventLog --st 20200601 --et 20200602 --
count 5 --file MaintenEventLog.txt --overwrite
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetMaintenEventLog
--file MaintenEventLog.txt --overwrite
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetMaintenEventLog
--count 5 --file MaintenEventLog.txt --overwrite
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetMaintenEventLog
--st 20200601 --et 20200602 --file MaintenEventLog.txt --overwrite
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetMaintenEventLog
--st 20200601 --et 20200602 --count 5 --file MaintenEventLog.txt --
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 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.

## 5.6.4. Getting Host Crash Dump Log



---

Use the “GetHostDump” command to have SAA show the managed system’s crash dump file.

- **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, SAA 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.
- 

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetHostDump --action <actiondump> [--file <HostDump.tgz> [--overwrite]]
In-Band	saa [-l <IP or host name> -u <username> -p <password>] -c GetHostDump --action <actiondump> [--file <HostDump.tgz> [--overwrite]]
Multiple Systems	

OOB	saa -l < system list file > [-u <username> -p <password>] -c GetHostDump --action <actiondump> [--file <HostDump.tgz> [--overwrite]]
-----	--------------------------------------------------------------------------------------------------------------------------------------

Example:

#### OOB:

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

#### In-Band:

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

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetHostDump --
action DeleteDump
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## 5.6.5. Clearing System Maintenance Event Log

Use the “ClearMaintenEventLog” command to execute SAA to clear the maintenance event log for the target system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ClearMaintenEventLog [--gen_log]
In-Band	saa -c ClearMaintenEventLog [--gen_log]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ClearMaintenEventLog [--gen_log]

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
ClearMaintenEventLog
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
ClearMaintenEventLog --gen_log
```

**In-Band:**

```
[SAA_HOME]# ./saa -c ClearMaintenEventLog
```

```
[SAA_HOME]# ./saa -c ClearMaintenEventLog --gen_log
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
ClearMaintenEventLog
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
ClearMaintenEventLog --gen_log
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

## 5.7. CMM Management (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.

### 5.7.1. 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetCmmInfo [--file <filename>]
In-Band	saa -c GetCmmInfo --file <filename> --file_only
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetCmmInfo [--file <filename>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCmmInfo --file Supermicro_CMM.bin
```

The console output contains the following information.

```
Managed system.....192.168.34.56
 CMM type.....MicroCMM
 CMM version.....09.01
 ARM SAA version.....1.0.0 (2021/12/10) (ARM)
 Dummy switch version.01.02
Local CMM image file....Supermicro_CMM.bin
 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 SAA version.....1.0.0 (2021/12/10) (ARM)
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetCmmInfo --file
Supermicro_CMM.bin
```

```
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.

## 5.7.2. Updating the CMM Firmware Image

Use the “UpdateCmm” command with the CMM firmware image Supermicro\_CMM.bin 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.
- 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.
- 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.
  - 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.)
  - 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.

---

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateCmm --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--overwrite_ssl] [--cmm_boot_check]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateCmm --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--overwrite_ssl] [--cmm_boot_check]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateCmm --file Supermicro.CMM.bin
```

---

## Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateCmm --file
Supermicro.CMM.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.

### 5.7.3. Getting CMM Settings

Use the “GetCmmCfg” command to execute SAA 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 5.5.16 Profile Update.
- 

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetCmmCfg [--file <CmmCfg.xml>] [--overwrite] [--download [-- profile_repo]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetCmmCfg --file <CmmCfg.xml> [--overwrite] [--download [-- profile_repo]]

Example:

---

**00B:**

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

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCmmCfg --
download --file CmmCfg.xml --overwrite
```

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

**Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -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.

### 5.7.4. Updating CMM Settings

1. Select one managed system as the golden sample for the current CMM settings.  
(For multiple systems)
2. Follow the steps in 5.7.3 Getting CMM settings.
3. Edit the configurable element values in the CMM configuration file CMMCfg.xml to the desired values as illustrated in 4.7.4 CMM Configuration Text 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 unchanged tables/elements in the text file. Note that this step is optional.
6. Use the command ChangeCmmCfg with the updated CMMCfg.xml file to run SAA to update the CMM configuration.



Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c ChangeCmmCfg --file &lt;CmmCfg.xml&gt; [--skip_unknown] [--precheck] saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c ChangeCmmCfg {--upload --file &lt;CmmCfg.xml&gt; [--skip_precheck]   -- update Apply   Deploy [--skip_unknown] [--precheck]}</pre>
Multiple Systems	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c ChangeCmmCfg --file &lt;CMMCfg.xml&gt; [--skip_unknown] [--precheck] [- -individually] saa -i &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c ChangeCmmCfg {--upload --file &lt;CmmCfg.xml&gt; [--skip_precheck]   -- update Apply   Deploy [--skip_unknown] [--precheck]}</pre>

Example:

#### OOB:

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

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

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

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeCmmCfg --
file CMMCfg.xml
```

```
[SAA_HOME]# ./saa -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. Then, name the --file argument as “CMMCfg.xml”. With the --individually option, SAA 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.



**Notes:**

- The connection might be lost if the LAN configuration is changed.
- The CMM configuration can be changed through 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” updates 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 multiple systems usage, 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 in multiple system usage.
- For profile update usage details, please refer to 5.5.16 Profile Update.
- The --skip\_unknown option is designed to skip all invalid tables and settings in the latest CMM configuration in the managed system.

---

### 5.7.5. Setting Up a CMM User Password

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

Single System	
OOB	saa -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>]}
In-Band	saa -c SetCmmPassword [--user_id <user ID>] [--new_password <new password> --confirm_password <confirm password>]   [--pw_file <password file path>]}
Multiple Systems	
OOB	saa -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:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmPassword
--user_id 3 --new_password 12345678 --confirm_password 12345678
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmPassword
--pw_file passwd.txt
```

#### In-Band:

```
[SAA_HOME]# ./saa -c SetCmmPassword --new_password 12345678 --
confirm_password 12345678
```

```
[SAA_HOME]# ./saa -c SetCmmPassword --user_id 3 --pw_file passwd.txt
```

```
passwd.txt:
CmmPasswordString
```

#### Multiple Systems OOB:

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetCmmPassword --
new_password 12345678 --confirm_password 12345678
```

```
[SAA_HOME]# ./saa -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
```

**Note:**

Without the --user\_id option, the user ID is set to 2 (as Administrator ) by default.

---

### 5.7.6 Loading the Factory CMM Settings

Use the “LoadDefaultCmmCfg” command to have SAA 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 5.5.9 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_p assword	N	Y	N	<b>ADMIN</b>
-- clear_user_cfg with --	N	Y	N	<b>Unique Password</b>

load_unique_password				
----------------------	--	--	--	--

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c LoadDefaultCmmCfg --preserve_user_cfg  saa -i <IP or host name> -u <username> -p <password> -c LoadDefaultCmmCfg --clear_user_cfg --load_unique_password  saa -i <IP or host name> -u <username> -p <password> -c LoadDefaultCmmCfg --clear_user_cfg --load_default_password
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c LoadDefaultCmmCfg --preserve_user_cfg  saa -l < system list file > [-u <username> -p <password>] -c LoadDefaultCmmCfg --clear_user_cfg --load_unique_password  saa -l < system list file > [-u <username> -p <password>] -c LoadDefaultCmmCfg --clear_user_cfg --load_default_password

Example:

#### OOB:

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

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

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

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultCmmCfg --preserve_user_cfg
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultCmmCfg --clear_user_cfg --load_unique_password
```

---

```
[SAA_HOME]# ./saa -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
```

**Notes:**

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

### 5.7.7 Getting BBP Firmware Image Information

Use the “GetBbpInfo” command to get the BBP firmware image and its information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBbpInfo [--file <filename>]
In-Band	saa -c GetBbpInfo [--file_only <filename>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetBbpInfo [--file <filename>]

Example:

**OOB:**

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

The console output contains the following information.

```

Managed system.....192.168.34.56
 BBP version.....01.08
Local BBP image file....BBP_EC_2019-03-14_1901.47v1.08.bin
 BBP version.....01.08

```

### Multiple OOB:

```
[SAA_HOME]# ./saa -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.

## 5.7.8 Updating the BBP Firmware Image

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateBbp --file <filename> [--skip_check]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateBbp --file <filename> [--skip_check]

Example:

### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBbp --
file BBP.bin
```

---

## Multiple OOB:

```
[SAA_HOME]# ./saa -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.



### 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.

---

## 5.7.9 Getting Current Power Status of Blade System

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBladePowerStatus
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetBladePowerStatus

Example:

**OOB:**



---

```
[SAA_HOME]# ./saa -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
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -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.

### **5.7.10 Setting the Power Status of the Blade System**

SAA 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SetBladePowerAction --action <action> --blade <Blade Index> [--node <Node Index>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SetBladePowerAction --action <action> --blade <Blade Index> [--node <Node Index>]

Option Commands	Descriptions
--action	Sets power action with: 0 = down 1 = up 2 = cycle 3 = reset 4 = softshutdown 24 = accycle
--blade	Assigns blade index [A1-A14], [B1-B14] or "ALL"
--node(optional)	Assigns node index [1-4]

Example:

#### OOB:

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

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SetBladePowerAction --blade ALL --action reset
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SetBladePowerAction --blade A1 --action softshutdown
```

#### Multiple OOB:

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
SetBladePowerAction --action down --blade ALL
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
SetBladePowerAction --blade ALL --action reset
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
SetBladePowerAction --blade A1 --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.

### 5.7.11 Managing the Profile Information

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

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

Single System	
OOB	saa -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]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ProfileManage --action <action> [--file <filename>]

Example:

---

**00B:**

```
[SAA_HOME]# ./saa -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.....192.168.34.56
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
```

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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.
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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.



#### **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 5.7.3 Getting CMM Settings.
- To upload the CMM configuration file, please use the ChangeCmmCfg command with the --upload option. For details, please refer to 5.7.4 Updating CMM Settings.
- To update the CMM configuration, please use the ChangeCmmCfg command with the --update option. For details, please refer to 5.7.4 Updating CMM Settings.

- To download the current system configuration file or system profile, please use the GetSystemCfg command with the --download option. For details, please refer to 5.3.3 Getting System Settings.
- To upload the system configuration file, please use the ChangeSystemCfg command with the --upload option. For details, please refer to 5.3.4 Updating the System Settings.

### 5.7.12 Receiving the Switch Firmware Image Information

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBladeSwitchInfo [--dev_id <Device ID>] [--file <filename>]
In-Band	saa -c GetBladeSwitchInfo --file <filename> --file_only
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBladeSwitchInfo [--dev_id <Device ID>] [--file <filename>]



#### 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 :

```
[SAA_HOME]# ./saa -c GetBladeSwitchInfo --file Supermicro_Switch.bin --file_only
```

#### OOB:

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetBladeSwitchInfo
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetBladeSwitchInfo --dev_id A1,A2
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetBladeSwitchInfo --file Supermicro_Switch.bin
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetBladeSwitchInfo --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
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBladeSwitchInfo

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetBladeSwitchInfo
--dev_id A1,A2 --file Supermicro_Switch.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.

## 5.7.13 Updating the Switch Firmware

Use the “UpdateBladeSwitch” 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 UpdateBladeSwitch command is executed. To reboot the switch module, execute the RebootBladeSwitch 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 GetBladeSwitchInfo command to get the switch device ID.

Single System	
OOB	<pre>saa -i &lt;Switch IP or switch host name&gt; -u &lt;Switch username&gt; -p &lt;Switch password&gt; -c UpdateBladeSwitch --file &lt;filename&gt; [--reboot] saa -i &lt;CMM IP or CMM host name&gt; -u &lt;CMM username&gt; -p &lt;CMM password&gt; -c UpdateBladeSwitch --file &lt;filename&gt; --dev_id &lt;Switch device ID&gt; --switch_user &lt;Switch username&gt; --switch_pw &lt;Switch password&gt; [--reboot]</pre>
Multiple Systems	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;Switch username&gt; -p &lt;Switch password&gt;] -c UpdateBladeSwitch --file &lt;filename&gt; [--reboot] [--individually] saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c UpdateBladeSwitch --file &lt;filename&gt; [--dev_id &lt;Switch device ID&gt; --switch_user &lt;Switch username&gt; --switch_pw &lt;Switch password&gt;] [--reboot] [--individually]</pre>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBladeSwitch --file Supermicro_Switch.bin --reboot
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBladeSwitch --file Supermicro_Switch.bin --dev_id A1 --switch_user ADMIN --switch_pw ADMIN --reboot
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SwitchList.txt -u ADMIN -p PASSWORD -c UpdateBladeSwitch --file Supermicro_Switch.bin --reboot
```

```
[SAA_HOME]# ./saa -l SwitchList.txt -u ADMIN -p PASSWORD -c UpdateBladeSwitch --file Supermicro_Switch.bin --reboot --individually
```

```
SwitchList.txt:
192.168.34.56
192.168.34.57
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateBladeSwitch
--file Supermicro_Switch.bin --dev_id A1 --switch_user ADMIN --switch_pw
ADMIN --reboot
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateBladeSwitch
--file Supermicro_Switch.bin --dev_id A1 --switch_user ADMIN --switch_pw
ADMIN --reboot --individually
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

For --individually 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, SAA 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.

## 5.7.14 Rebooting the Switch

Use the “RebootBladeSwitch” 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 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.
- 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 GetBladeSwitchInfo command to get the switch device ID.

Single System	
OOB	<pre>saa -i &lt;Switch IP or switch host name&gt; -u &lt;Switch username&gt; -p &lt;Switch password&gt; -c RebootBladeSwitch saa -i &lt;CMM IP or CMM host name&gt; -u &lt;CMM username&gt; -p &lt;CMM password&gt; -c RebootBladeSwitch --dev_id &lt;Switch device ID&gt; --switch_user &lt;Switch username&gt; --switch_pw &lt;Switch password&gt;</pre>
Multiple Systems	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;Switch username&gt; -p &lt;Switch password&gt;] -c RebootBladeSwitch saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c RebootBladeSwitch [--dev_id &lt;Switch device ID&gt; --switch_user &lt;Switch username&gt; --switch_pw &lt;Switch password&gt;]</pre>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
RebootBladeSwitch
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
RebootBladeSwitch --dev_id A1 --switch_user ADMIN --switch_pw
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SwitchList.txt -u ADMIN -p PASSWORD -c
RebootBladeSwitch
```

```
[SAA_HOME]# ./saa -l SwitchList.txt -u ADMIN -p PASSWORD -c
RebootBladeSwitch --dev_id A1 --switch_user ADMIN --switch_pw ADMIN
```

```
SwitchList.txt:
192.168.34.56
192.168.34.57
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateBladeSwitch
--file Supermicro_Switch.bin --dev_id A1 --switch_user ADMIN --switch_pw
ADMIN --reboot
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateBladeSwitch
--file Supermicro_Switch.bin --dev_id A1 --switch_user ADMIN --switch_pw
ADMIN --reboot --individually
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## 5.7.15. Blade Power Supply Unit Management

BladePsuManage command can manage blade power supply unit (PSU) for Supermicro Blade systems.

The following table summarizes the supported actions in BladePsuManage command.

Option	--action
Description	GetBladePsuInfo = Display Blade PSU Information GetBladePsuConsumption = Display power consumption of Blade system power supply module GetFanSpeed = Get Blade system fan speed SetFanSpeed = Set Blade system fan speed GetFanMode= Get Blade system fan mode SetFanMode = Set Blade system fan mode

### 5.7.15.1. Getting Blade Power Supply Unit Information

Use the BladePsuManage command with option --action GetBladePsuInfo to get power supply unit (PSU) information from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladePsuManage --action GetBladePsuInfo
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action GetBladePsuInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BladePsuManage
--action GetBladePsuInfo
```

The console output contains the following information.

```
PSU A1
=====
Item | Value
---- | ----
Power Supply | Power Supply A1
Model Name | PWS-DF006-2F
Power Status | On
Temperature (°C) | 45
Fan1 Speed (RPM) | 10877
Fan2 Speed (RPM) | 11793
AC Input Voltage | N/A
Max Watt | N/A
AC Input Current | N/A
DC Output Current | N/A
Current Power Usage | N/A
FW Version | 1.0
FRU Version | 1
Error | Normal

PSU A2
=====
Item | Value
---- | ----
Power Supply | Power Supply A2
Model Name | PWS-2K21A-BR
Power Status | On
Temperature (°C) | 44
Fan1 Speed (RPM) | 12137
```

Fan2 Speed (RPM)		11106
AC Input Voltage		117 V
Max Watt		1200 W
AC Input Current		3.19 A
DC Output Current		20 A
Current Power Usage		20.00 %
FW Version		1.0
FRU Version		1
Error		Normal

#### PSU A3

=====

Item		Value
----		-----
Power Supply		Power Supply A3
Model Name		PWS-2K21A-BR
Power Status		On
Temperature (°C)		45
Fan1 Speed (RPM)		11793
Fan2 Speed (RPM)		11106
AC Input Voltage		117 V
Max Watt		1200 W
AC Input Current		3.12 A
DC Output Current		20 A
Current Power Usage		20.00 %
FW Version		1.0
FRU Version		1
Error		Normal

#### PSU A4

=====

Item		Value
----		-----
Power Supply		Power Supply A4
Model Name		PWS-DF006-2F
Power Status		On
Temperature (°C)		45
Fan1 Speed (RPM)		11106
Fan2 Speed (RPM)		11908
AC Input Voltage		N/A
Max Watt		N/A
AC Input Current		N/A
DC Output Current		N/A
Current Power Usage		N/A
FW Version		1.0
FRU Version		1
Error		Normal

#### PSU B1

=====

Item	Value
----	-----
Power Supply	Power Supply B1
Model Name	PWS-DF006-2F
Power Status	On
Temperature (°C)	45
Fan1 Speed (RPM)	10992
Fan2 Speed (RPM)	11793
AC Input Voltage	N/A
Max Watt	N/A
AC Input Current	N/A
DC Output Current	N/A
Current Power Usage	N/A
FW Version	1.0
FRU Version	1
Error	Normal

#### PSU B2

=====

Item	Value
----	-----
Power Supply	Power Supply B2
Model Name	PWS-2K21A-BR
Power Status	On
Temperature (°C)	45
Fan1 Speed (RPM)	11564
Fan2 Speed (RPM)	11106
AC Input Voltage	117 V
Max Watt	1200 W
AC Input Current	3.19 A
DC Output Current	20 A
Current Power Usage	20.00 %
FW Version	1.0
FRU Version	1
Error	Normal

#### PSU B3

=====

Item	Value
----	-----
Power Supply	Power Supply B3
Model Name	PWS-2K21A-BR
Power Status	On
Temperature (°C)	45
Fan1 Speed (RPM)	11679
Fan2 Speed (RPM)	10992
AC Input Voltage	116 V
Max Watt	1200 W
AC Input Current	3.38 A
DC Output Current	22 A
Current Power Usage	22.00 %

FW Version		1.0
FRU Version		1
Error		Normal

#### PSU B4

=====

Item		Value
----		-----
Power Supply		Power Supply B4
Model Name		PWS-DF006-2F
Power Status		On
Temperature (°C)		44
Fan1 Speed (RPM)		10992
Fan2 Speed (RPM)		11679
AC Input Voltage		N/A
Max Watt		N/A
AC Input Current		N/A
DC Output Current		N/A
Current Power Usage		N/A
FW Version		1.0
FRU Version		1
Error		Normal

#### Fan C1

=====

Fan		Fan C1
Model Name		N/A
Power Status		N/A
Fan1 Speed (RPM)		N/A
Fan2 Speed (RPM)		N/A
Fan3 Speed (RPM)		N/A

#### Fan C2

=====

Fan		Fan C2
Model Name		N/A
Power Status		N/A
Fan1 Speed (RPM)		N/A
Fan2 Speed (RPM)		N/A
Fan3 Speed (RPM)		N/A

#### Fan C3

=====

Fan		Fan C3
Model Name		N/A
Power Status		N/A
Fan1 Speed (RPM)		N/A



Fan2 Speed (RPM)		N/A
Fan3 Speed (RPM)		N/A

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladePsuManage --
action GetBladePsuInfo
```

```
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.

### 5.7.15.2. Getting Blade Power Supply Unit Consumption

Use the BladePsuManage command with option --action GetBladePsuConsumption to get power consumption of Blade system power supply module from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladePsuManage --action GetBladePsuConsumption
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action GetBladePsuConsumption

Example:

### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BladePsuManage
--action GetBladePsuConsumption
```

The console output contains the following information.

Module	Power Consumption (W)
PS A1	195
PS A2	208
PS A3	207
PS A4	209
PS B1	222
PS B2	222
PS B3	194
PS B4	221
Total	1678

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladePsuManage --
action GetBladePsuConsumption
```

```
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.

### 5.7.15.3. Getting Blade System Fan Speed

Use the BladePsuManage command with option --action GetFanSpeed to get Blade system fan speed from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladePsuManage --action GetFanSpeed
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action GetFanSpeed

---

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BladePsuManage
--action GetFanSpeed
```

**The console output contains the following information.**

Current Fan Speed Level: 5

**Multiple Systems OoB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladePsuManage --
action GetFanSpeed
```

```
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.

#### 5.7.15.4. Setting Blade System Fan Speed

Use the BladePsuManage command with option --action SetFanSpeed to set Blade system fan speed from managed system.

The following is the supported options for option --action SetFanSpeed.

Option	Description
--value	Assigns fan speed level. Speed level: [1-10]

Single System	
OoB	saa -i <IP or host name> -u <username> -p <password> -c

	BladePsuManage --action SetFanSpeed --value <value>
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action SetFanSpeed --value <value>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BladePsuManage --action SetFanSpeed --value 5
```

The console output contains the following information.

```
BladePsuManage command is completed.
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladePsuManage --action SetFanSpeed --value 5
```

```
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.

#### 5.7.15.5. Getting Blade System Fan Mode

Use the BladePsuManage command with option --action GetFanMode to get Blade system fan mode from managed system.

<b>Single System</b>	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladePsuManage --action GetFanMode

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action GetFanMode

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BladePsuManage --action GetFanMode
```

The console output contains the following information.

```
Current Fan Mode: Manual
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladePsuManage --action GetFanMode
```

```
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.

#### 5.7.15.6. Setting Blade System Fan Mode

Use the BladePsuManage command with option --action SetFanMode to set Blade system fan mode from managed system.

The following is the supported options for option --action SetFanMode.

Option	Description
--------	-------------

--value	Assigns fan mode. 0: Auto 1: Manual
---------	-------------------------------------------

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladePsuManage --action SetFanMode --value <value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action SetFanMode --value <value>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BladePsuManage
--action SetFanMode --value 0
```

The console output contains the following information.

```
BladePsuManage command is completed.
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladePsuManage --
action SetFanMode --value 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.

## 5.7.16 Profile Management

---

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
Profile Manage	<ul style="list-style-type: none"><li>Gets and edits profile information or deletes the profile on CMM</li><li>Provides profile association information between specified profile and the selected Blade systems.</li></ul>
GetCmmCfg	Downloads the current repository CMM configuration from CMM.
ChangeCmmCfg	<ul style="list-style-type: none"><li>Uploads the CMM configuration to CMM.</li><li>Updates the CMM configuration to CMM by the existing CMM configuration on CMM.</li></ul>
GetSystemCfg	Downloads the current or repository system configuration from CMM.
ChangeSystemCfg	<ul style="list-style-type: none"><li>Uploads the CMM configuration to CMM.</li><li>Updates the system configuration to a Blade system through CMM with the existing system configuration on CMM.</li></ul>

#### 5.7.16.1 Profile Update Rule

SAA 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.



---

### 5.7.16.2. 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 5.7.11 Managing the profile Information.
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 5.7.11 Managing the profile Information.
4. Execute ProfileManage command with the --Action Get option again to check whether the profile information is changed. For more details, please refer to 5.7.11 Managing the profile Information.

### 5.7.16.3. 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 5.7.11 Managing the profile Information.
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 5.7.3 Getting CMM Settings.
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 5.7.4 Updating CMM Settings.
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 5.7.11 Managing the profile Information.
  6. Execute the ChangeCmmCfg command with the --Update option to update the selected CMM configuration the profile. For more details, please refer to 5.7.4 Updating CMM 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 5.7.11 Managing the profile Information.



**Note:**

Use the ProfileManage command to upload the profile information to CMM, which can be updated. Please refer to 5.7.11 Managing the Profile Information.

---

#### 5.7.16.4. Updating Blade System 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 5.7.11 Managing the profile Information.
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 5.3.3 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 5.7.11 Managing the profile Information.
6. 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 5.3.4 Updating System Settings.

- 
7. 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 5.7.11 Managing the profile Information.
- 



**Note:**

Use the ProfileManage command to upload the profile information to CMM, which can be updated later. Please refer to 5.7.11 Managing the Profile Information.

---

### 5.7.17 Getting Blade Summary

BladeSummary command can get all Blade summary information for all Supermicro Blade systems.

---



**Notes:**

- Fan information will only be displayed if the CMM Middle Plane is 820 series.
  - To check CMM Middle Plane information, please refer to 5.3.1.1 Getting FRU Information.
- 

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeSummary
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeSummary

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BladeSummary
```

**The console output contains the following information.**

---

#### Blade Module (5/28)

```

Blade | Status
----- | -----
A1 | Normal
 |
 | Node | BMC IP | Status
 | ---- | -
 | 1 | 12.34.56.78 | Normal
A2 | Normal
 |
 | Node | BMC IP | Status
 | ---- | -
 | 1 | 12.34.56.78 | Normal
A3 | Normal
 |
 | Node | BMC IP | Status
 | ---- | -
 | 1 | 12.34.56.78 | Normal
A5 | Normal
 |
 | Node | BMC IP | Status
 | ---- | -
 | 1 | 12.34.56.78 | Normal
A7 | Normal
 |
 | Node | BMC IP | Status
 | ---- | -
 | 1 | 12.34.56.78 | Normal
```

#### Switch Module (3/4)

```

Switch | Status
----- | -----
A1 | On
A2 | On
B1 | On
```

#### Power Supply Module (8/8)

```

Power Supply | Status
----- | -----
A1 | Normal
A2 | Normal
A3 | Normal
A4 | Normal
B1 | Normal
B2 | Normal
B3 | Normal
B4 | Normal
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeSummary
```

```
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.

### 5.7.18. Getting the CMM User List

Use the “GetCmmUserList” command to get the current CMM user list from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetCmmUserList
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetCmmUserList

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCmmUserList
```

**The console output contains the following information.**

```
Maximum number of Users : 16
Count of currently enabled Users : 1
User ID | User Name | Privilege Level | Enabled | Account Types
===== | ===== | ===== | ===== | =====
 2 | ADMIN | Administrator | Yes | Redfish/IPMI
===== | ===== | ===== | ===== | =====

The CMM user list.
```

**Multiple Systems OOB:**

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetCmmUserList
```

```
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.

### 5.7.19. Setting the CMM User List

Use the “SetCmmUserList” command to set the current CMM user list for the target system.

- **Add new CMM user**

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

- **Delete the CMM user**

Use the “SetCmmUserList” command with the “--action Del” option to delete a CMM user.

- **Change a CMM user's privilege**

Use the “SetCmmUserList” command with the “--action Level” option to change a CMM user's privilege.

- **Change a CMM user password**

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

- **Test CMM user login**

Use the “SetCmmUserList” command with the “--action Test” option to verify a CMM user login.

- **Enable the CMM user type**

Use the “SetCmmUserList” command with the “--action EnableType” option to activate a CMM user type.

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetCmmUserList --action add --user_id &lt;userid&gt; --user_name &lt;username&gt; --user_password &lt;userpassword&gt; --user_privilege &lt;userprivilege&gt;  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetCmmUserList --action &lt;action&gt; --user_id &lt;userid&gt; [--user_name &lt;username&gt;] [--user_password &lt;userpassword&gt;] [--user_privilege &lt;userprivilege&gt;]  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetCmmUserList --action Test --user_name &lt;username&gt; -- user_password &lt;userpassword&gt;  saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetCmmUserList --action EnableType --user_id --account_type &lt;type&gt; --account_type_status &lt;status&gt; [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]</pre>
Multiple Systems	
OOB	<pre>saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetCmmUserList --action add --user_id &lt;userid&gt; --user_name &lt;username&gt; --user_password &lt;userpassword&gt; --user_privilege &lt;userprivilege&gt;  saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetCmmUserList --action &lt;action&gt; --user_id &lt;userid&gt; [--user_name &lt;username&gt;] [--user_password &lt;userpassword&gt;] [--user_privilege &lt;userprivilege&gt;]  saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetCmmUserList --action Test --user_name &lt;username&gt; -- user_password &lt;userpassword&gt;  saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetCmmUserList --action EnableType --user_id --account_type &lt;type&gt;</pre>

---

	<code>--account_type_status &lt;status&gt; [--ap &lt;protocol&gt; --pp &lt;protocol&gt; --ak &lt;key&gt; --pk &lt;key&gt;]</code>
--	-----------------------------------------------------------------------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmUserList
--action Add --user_id 3 --user_name NAME3 --user_password PASSWORD3 --
user_privilege 3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmUserList
--action Del --user_id 3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmUserList
---action Level --user_id 3 --user_privilege 3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmUserList
--action SetPwd --user_id 3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmUserList
--action Test --user_name NAME3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetCmmUserList
--action EnableType --user_id 3 --account_type SNMP --account_type_status
enable --ap 0 --pp DES --ak KEY --pk KEY
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetCmmUserList --
action Add --user_id 3 --user_name NAME3 --user_password PASSWORD3 --
user_privilege 3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetCmmUserList --
action Del --user_id 3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetCmmUserList ---
action Level --user_id 3 --user_privilege 3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetCmmUserList --
action SetPwd --user_id 3 --user_password PASSWORD3
```



---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetCmmUserList --
action Test --user_name NAME3 --user_password PASSWORD3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetCmmUserList --
action EnableType --user_id 3 --account_type SNMP --account_type_status
enable --ap 0 --pp DES --ak KEY --pk KEY
```

```
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:**

- The "No Access" user privilege is not supported on platforms after the AST2600 series.
  - The "--action EnableType are not supported on platforms before the AST2600 series.
- 

## 5.7.20 Updating Dummy Switch Firmware Image

Use the “UpdateDummySwitch” command with the dummy switch firmware image to update dummy switch firmware on a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateDummySwitch [--file <filename> [--upload]   update <Apply>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateDummySwitch [--file <filename> [--upload]   update <Apply>] [--individually]

Example:

---

## OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateDummySwitch --file DummySwitch.rom
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateDummySwitch --file DummySwitch.rom --upload
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateDummySwitch --update Apply
```

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateNICCpld --
file DummySwitch.rom
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateDummySwitch
--file DummySwitch.rom --upload
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateDummySwitch
--update Apply
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## 5.8. Storage Management

### 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.

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c GetRaidControllerInfo [--file &lt;filename&gt;] [--controller &lt;Broadcom Marvell&gt;] [--dev_id &lt;controller_id&gt;]</pre>

In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetRaidControllerInfo [--file <filename> [--file_only]] [--controller <Broadcom Marvell>] [--dev_id <controller_id>]
<b>Multiple Systems</b>	
OOB	saa -I <system list file> [-u <username> -p <password>] -c GetRaidControllerInfo [--file <filename>] [--controller <Broadcom Marvell>] [--dev_id <controller_id>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetRaidControllerInfo --file RAID.rom
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
GetRaidControllerInfo --file RAID.rom
```

The console output contains the following information.

```
Managed System.....192.168.34.56
Device ID.....Device 0
Product Name.....AVAGO 3108 MegaRAID
Serial.....N/A
Package.....24.18.0-0021
Firmware Version.....4.670.00-6500
BIOS Version.....6.34.01.0_4.19.08.00_0x06160200
Boot Block Version.....3.07.00.00-0003
Local RAID Firmware Image File.....AVAGO_3108_4.680.00-8290.rom
Product Name.....AVAGO 3108 MegaRAID
Package.....24.21.0-0028
Firmware Version.....4.680.00-8290
BIOS Version.....6.36.00.2_4.19.08.00_0x06180202
Boot Block Version.....3.07.00.00-0003
```

#### In-Band:

```
[SAA_HOME]# ./saa -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
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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.

## 5.8.2. Updating the RAID Firmware Image

Use the command UpdateRaidController with RAID firmware image RAID.rom to update the managed system.



### Notes:

- The “UpdateRaidController” command only supports Broadcom 3108, 3408, 3808, 3816, 3908, 3916, 4116, and Marvell SE9230.
- Broadcom 3108 is supported by the following firmware images: RAID firmware image of version 4.650.00-8095 and later.
- Starting with X12 platforms and later, the --type option is required when using the Broadcom controller.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateRaidController --file <filename> --controller

	<Broadcom Marvell> [--type <HBA HA-RAID>] --dev_id <controller_id> [--reboot]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c UpdateRaidController --file <filename> --controller <Broadcom Marvell> [--type <HBA HA-RAID>] --dev_id <controller_id> [--reboot]
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateRaidController --file <filename> --controller <Broadcom Marvell> [--type <HBA HA-RAID>] --dev_id <controller_id> [--reboot]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateRaidController --controller Broadcom --type HA-RAID --dev_id 0 --
file RAID.rom --reboot
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
UpdateRaidController --controller Marvell --dev_id 0 --file RAID.rom --
reboot
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
UpdateRaidController --controller Broadcom --type HA-RAID --dev_id 0 --
file RAID.rom --reboot
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### 5.8.3. Getting RAID Settings

---

Use the “GetRaidCfg” command to execute SAA to get the current RAID settings from the managed system and save it in the RAIDCfɡ.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 SAA cannot get or change the RAID configurations of JBOD mode setting under the Controller Properties in an in-band environment.
- 

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetRaidCfg --file <filename> [--overwrite]
In-Band	saa -c GetRaidCfg --file <filename> [--overwrite]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetRaidCfg --file <filename> [--overwrite]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetRaidCfg --file RAIDCfɡ.xml
```

**In-Band:**

```
[SAA_HOME]# ./saa -c GetRaidCfg --file RAIDCfɡ.xml --overwrite
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetRaidCfg --file RAIDCfɡ.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.

### 5.8.4. Updating the RAID Settings

1. Select one managed system as the golden sample for current RAID settings. (For multiple systems usage)
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 4.7.5 RAID 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 “ChangeRaidCfg” command with the updated RAIDCfg.xml file to run SAA to update the RAID configuration.



#### Notes:

- For multiple systems usage, 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.
  - 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
  - The SAA cannot get or change the RAID configurations of JBOD mode setting under the Controller Properties in an in-band environment.
-

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChangeRaidCfg --file <filename>
In-Band	saa -c ChangeRaidCfg --file <filename>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeRaidCfg --file <filename>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeRaidCfg
--file RAIDCfG.xml
```

#### In-Band:

```
[SAA_HOME]# ./saa -c ChangeRaidCfg --file RAIDCfG.xml
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeRaidCfg --
file RAIDCfG.xml
```

```
[SAA_HOME]# ./saa -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, SAA 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.

### 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSataInfo
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetSataInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetSataInfo
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

### 5.8.6. Getting NVMe Information

Use the “GetNvmeInfo” command to get the current NVMe information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetNvmeInfo [--dev_id <device_id>]
In-Band	saa -c GetNvmeInfo [--dev_id <device_id>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetNvmeInfo [ --dev_id <device_id>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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)]
 Name: vmhba1
```

---

```
Slot: 0
Temperature: 51 degree C
Capacity: 1000 GB
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: S1N0NYAF800079
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
```

If TAS is not installed on machine, it will display "Please install TAS" instead.  
**The console output contains the following information.**

```
NVMe Device information
=====
[NVMe Controller(1)]
 Device ID: 0
 [Group(1)]
 Group ID: 0
 [NVMe SSD(1)]
 Name: Please install TAS
 Slot: 0
 Temperature: 51 degree C
 Capacity: Please install TAS
 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: S1N0NYAF800079
 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
```

**Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetNvmeInfo
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

### 5.8.7 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).

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetPMemInfo [--file <filename>]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c GetPMemInfo [--file <filename>] saa -c GetPMemInfo --file <filename> --file_only
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetPMemInfo [--file <filename>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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 :

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -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.



### Notes:

- This command is available on X12 3rd Gen Intel® Xeon® Scalable processors with Intel® C621A Series Chipsets and later platforms.
- The PMem firmware version retrieved from the “GetPMemInfo” command is the running PMem firmware version.

- For more detailed usages of PMem, please contact Supermicro technical support.

### 5.8.8 Updating the PMem Firmware Image

Use the “UpdatePMem” command with the PMem firmware image PMem.bin to run SAA to update the PMem of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdatePMem [--file <filename>   --restore_default_fw] [--current_password <current password>   --cur_pw_file <current password file path>] [--reboot [--post_complete]]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c UpdatePMem --file <filename> [--reboot] saa -c UpdatePMem --restore_default_fw [--current_password <current password>   --cur_pw_file <current password file path>] [--reboot]
Multiple Systems	
OOB	saa -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 [--post_complete]]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdatePMem --file PMem.bin --reboot
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
 PMem version.....2.2.0.1464
Local PMem image file.....PMem.bin
 PMem version.....2.2.0.1469
```

---

```
Status: Start uploading PMem firmware for 192.168.34.56
```

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

```

```
Status: PMem firmware is updated for 192.168.34.56
```

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

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

```
Status: PMem is updated for 192.168.34.56
```

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

### **In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdatePMem --file
PMem.bin --reboot
```

```
[SAA_HOME]# ./saa -c UpdatePMem --restore_default_fw --reboot
```

### **The console output contains the following information.**

```
Managed system.....169.254.3.254
 PMem version.....2.2.0.1464
Local PMem image file.....Local PMem image file
 PMem version.....2.2.0.1469
```

```
Status: Start updating PMem firmware for the managed system
```

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

```

```
Status: PMem firmware is updated for the managed system
```

```
System will reboot now.
System reboot command issued.
```

### **Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -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.



**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 Supermicro technical support.

---

### 5.8.9. Getting VROC Settings

Use the “GetVROCCfg” command to execute SAA 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 the BIOS setting needs to be set to “VMD” in order to use “GetVROCCfg” command.
- Host software in target system OS is required for VROC related commands.
- The Target system needs to boot into the OS in order to use VROC related commands.
- VROC related commands must have been tested on Red Hat Enterprise Linux 8.1.

---

Single System
---------------



OOB	saa -i <IP or host name> -u <username> -p <password> -c GetVROCCfg --file <filename> [--overwrite]
In-Band	saa -c GetVROCCfg --file <filename> [--overwrite]
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetVROCCfg --file <filename> [--overwrite]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetVROCCfg --file VROC.cfg.xml
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GetVROCCfg --file VROC.cfg.xml --overwrite
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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 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. 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.

### 5.8.10. Updating the VROC Settings

1. Follow the steps in 5.8.9 Getting VROC Settings.
2. Edit the configurable element values in the VROC configuration XML file VROC.cfg.xml, as illustrated in 4.7.6 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 SAA to update the VROC configuration.



**Note:**

Use the --individually option to update each managed system with the corresponding configuration file concurrently. The --individually option is required for this command.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChangeVROCCfg --file <filename>
In-Band	saa -c ChangeVROCCfg --file <filename>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeVROCCfg --file <filename>

Example:

**OOB:**

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

**In-Band:**

```
[SAA_HOME]# ./saa -c ChangeVROCCfg --file VROC.cfg.xml
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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 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 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, SAA 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.

### 5.8.11. Controlling an 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. However, if you are using the “Rescan” action, you don’t need to provide parameters. Please see 5.8.6 Getting NVMe Information 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.
- **Rescan:** rescans the device (Note that this function is only available on systems with TAS installed).

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ControlNvme --action <action> --dev_id <device ID> --group_id <group ID> --slot <slot number>

In-Band	saa -c ControlNvme --action <action> --dev_id <device ID> --group_id <group ID> --slot <slot number>
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c ControlNvme --action <Action> --dev_id <device ID> --group_id <group ID> --slot <slot num>

Example:

#### OOB:

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

```
[SAA_HOME]# ./saa -i 192.168.3.4 -u ADMIN -p PASSWORD -c ControlNVMe --
action Rescan
```

#### In-band:

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

```
[SAA_HOME]# ./saa -c ControlNVMe --action Rescan
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ControlNvme --
action Locate --dev_id 0 --group_id 0 --slot 0
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ControlNvme --
action Rescan
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## 5.8.12. Getting NVMe Smart Data

Use the “GetSmartData” command to get NVMe smart data information.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSmartData -- device_name <DEVICE_NAME>
In-Band	saa -c GetSmartData --device_name <DEVICE_NAME>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetSmartData

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSmartData -
- device_name vmhba1
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GetSmartData --device_name vmhba1
```

The console output contains the following information.

```
[Device name : vmhba1]
Critical warning : 0
IB Temp. : 324 K
Available spare : 99 %
Available spare threshold : 10 %
Percentage used : 0 %
Data units read (512k bytes) : 0x84c55b
Data units written (512k bytes) : 0x1734d9
Host read commands : 0x6ed1332
Host write commands : 0x1234ee2
Controller busy time (minutes) : 0x8
Power cycles : 0x38e8
Power on hours : 0x2df3
Unsafe shutdowns : 0x2a20
Media errors : 0x0
Error log entries : 0x0
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetSmartData
```

```
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.

### 5.8.13. Getting SAS Expander Firmware Image Information

Use the “GetSasExpanderInfo” command to obtain both the SAS Expander firmware image and its corresponding information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSasExpanderInfo [--file <filename>]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c GetSasExpanderInfo [--file <filename>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetSasExpanderInfo [--file <filename>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetSasExpanderInfo --file BPN_SAS3.rom
```

```
Managed system.....192.168.34.56
[SAS Expander 1]
 SAS Expander Name.....SASExpander Device 0
 SAS Expander Version.....99.25.01.02
Local SAS Expander image file.....BPN_SAS3.rom
 SAS Expander Name.....826SE1
 SAS Expander Version.....00.25.00.01
```

### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
GetSasExpanderInfo
```

```
Managed system.....169.254.3.254
[SAS Expander 1]
SAS Expander Name.....SASExpander Device 0
SAS Expander Version.....00.25.00.01
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetSasExpanderInfo
```

```
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.

## 5.8.14. Updating SAS Expander Firmware Image

Use the “UpdateSasExpander” command with the SAS Expander firmware image SAS\_FW.rom to run SAA to update the SAS Expander of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateSasExpander --file <filename> --index 1 [--reboot]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateSasExpander --file <filename> --index 1 [--reboot]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateSasExpander --file <filename> --index 1 [--reboot]

Example:

---

## OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateSasExpander --file SAS_FW.rom --index 1 --reboot
```

## In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateSasExpander
--file SAS_FW.rom --index 1
```

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateSasExpander
--file SAS_FW.rom --index 1
```

```
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.

## 5.9. Power Management

### 5.9.1. Getting PSU Information

Use the “GetPsuInfo” command to get the current PSU information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetPsuInfo
In-Band	saa -c GetPsuInfo
Multiple Systems	



---

OOB	saa -l <system list file> -u <username> -p <password> -c GetPsuInfo
-----	---------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetPsuInfo
```

**In-Band:**

```
[SAA_HOME]# ./saa -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
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetPsuInfo
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

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.

---

## 5.9.2. 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 SAA to update the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdatePsu --file <filename> --address <PSU slave address>
In-Band	saa -c UpdatePsu --file <filename> --address <PSU slave address>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdatePsu --file <filename> --address <PSU slave address>

Example:

### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdatePsu --file Supermicro_PSU.x0 --address 0x80
```

### In-Band:

```
[SAA_HOME]# ./saa -c UpdatePsu --file Supermicro_PSU.x0 --address 0x80
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD --c UpdatePsu --file Supermicro_PSU.x0 --address 0x80
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

---

### 5.9.3. Getting Current Power Status of a Managed System

Use the “GetPowerStatus” command to get the current power status of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetPowerStatus
In-Band	saa -c GetPowerStatus
Multiple System	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetPowerStatus

Example:

#### OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -c GetPowerStatus
```

The console output contains the following information.

```
Managed system.....localhost
Power status.....On
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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 BIOS and BMC capabilities of the managed system will be shown in the “Execution Message” section in the created log file.

### 5.9.4. Setting the Power Action of a Managed System

Use the “SetPowerAction” command to set the type of power action of the managed system.

Command Options	Descriptions
--action	Sets action to:  0 = up  1 = down  2 = cycle  3 = reset  4 = softshutdown  5 = reboot  6 = accycle

Syntax of SetPowerAction:

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SetPowerAction --action <action> [--interval <time interval>] [--post_complete]
In-Band	saa -c SetPowerAction --action <action> [--interval <time interval>]
Multiple System	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SetPowerAction --action <action> [--interval <time interval>] [--

---

	post_complete]
--	----------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetPowerAction --action up
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetPowerAction --action 0
```

**In-Band:**

```
[SAA_HOME]# ./saa -c SetPowerAction --action up
```

```
[SAA_HOME]# ./saa -c SetPowerAction --action 0
```

**The console output contains the following information.**

```
Proceeding to power up the managed system.
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetPowerAction --action up
```

```
[SAA_HOME]# ./saa -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 BIOS and BMC capabilities of the managed system will be shown in the “Execution Message” section in the created log file.

### 5.9.5. Getting ACPI Power Status of a Managed System

---

Use the “GetAcpiPowerStatus” command to get the current ACPI (Advanced Configuration and Power Interface) status of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetAcpiPowerStatus
In-Band	saa -c GetAcpiPowerStatus
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetAcpiPowerStatus

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetAcpiPowerStatus
```

**In-Band:**

```
[SAA_HOME]# ./saa -c GetAcpiPowerStatus
```

**The console output contains the following information.**

```
ACPI Power Status: S0/G0 Working
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetAcpiPowerStatus
```

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.

### 5.9.6. Managing Intel Node Manager Policy

PowerPolicy command can manage power policy by Intel Intelligent Power Node Manager (NM) or BMC Intel Node Manager (BMC-NM) for Supermicro Intel platforms.

The following table summarizes the supported actions in PowerPolicy command with each NM or BMC-NM version.

Option	--type	--action
Description	NM20 = Node manager 2.0	EnableGlobal = Enables NM policy control Globally DisableGlobal = Disables NM policy control Globally EnableDomain = Enables NM policies for specified domain DisableDomain = Disables NM policies for specified domain EnablePolicy = Enables specified NM policy DisablePolicy = Disables specified NM policy AddPowerPolicy = Adds power policy GetPolicy = Gets policy DelPolicy = Deletes policy ScanPolicy = Scans all presented policies AddPolicy = Adds policy GetAlertThreshold = Gets policy alert thresholds SetAlertThreshold = Sets policy alert thresholds GetPeriod = Displays suspension period AddPeriod = Adds suspension period UpdatePeriod = Updates suspension period DeletePeriod = Deletes suspension period ClearPeriod = Clears suspension period
	BMC10 = BMC Intel Node Manager 1.0	EnableGlobal = Enables NM policy control Globally DisableGlobal = Disables NM policy control Globally EnableDomain = Enables NM policies for specified domain DisableDomain = Disables NM policies for specified domain EnablePolicy = Enables specified NM policy DisablePolicy = Disables specified NM policy AddPowerPolicy = Adds power policy GetPolicy = Gets policy DelPolicy = Deletes policy

		ScanPolicy = Scans all presented policies AddPolicy = Adds policy
--	--	----------------------------------------------------------------------



**Note:** Starting from X14 and later platforms, please use the --type BMC10 option instead of NM20. These platforms do not have a Management Engine (ME) to support Intel Node Manager management.

### 5.9.6.1. Managing the Power Policy by Intel Intelligent Power Node Manager

#### 5.9.6.1.1 Enabling Node Manager Policy Control Globally

Use the PowerPolicy command with option --action EnableGlobal to enable NM policy control globally of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action EnableGlobal
In-Band	saa -c PowerPolicy --type NM20 --action EnableGlobal
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action EnableGlobal

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action EnableGlobal
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action EnableGlobal
```

#### Multiple OOB:



---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action EnableGlobal
```

```
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.

#### 5.9.6.1.2. Disabling Node Manager Policy Control Globally

Use the PowerPolicy command with option --action DisableGlobal to disable NM policy control globally of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action DisableGlobal
In-Band	saa -c PowerPolicy --type NM20 --action DisableGlobal
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action DisableGlobal

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DisableGlobal
```

##### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action DisableGlobal
```

##### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DisableGlobal
```

```
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.

#### 5.9.6.1.3. Enabling Node Manager Policies for Specified Domain

Use the PowerPolicy command with option `--action EnableDomain` to enable NM policies for specified domain of a managed system.

The following is the supported option for option `--action EnableDomain`.

Option	Description
<code>--domain_id</code>	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type NM20 --action EnableDomain --domain_id &lt;domain ID&gt;</code>
In-Band	<code>saa -c PowerPolicy --type NM20 --action EnableDomain --domain_id &lt;domain ID&gt;</code>
Multiple Systems	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type NM20 --action EnableDomain --domain_id &lt;domain ID&gt;</code>

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action EnableDomain --domain_id 0
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action EnableDomain --domain_id 0
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action EnableDomain --domain_id 0
```

```
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.

#### **5.9.6.1.4. Disabling Node Manager Policies for Specified Domain**

Use the PowerPolicy command with option --action DisableDomain to disable NM policies for specified domain of a managed system.

The following is the supported option for option --action DisableDomain.

Option	Description
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action DisableDomain --domain_id <domain ID>
In-Band	saa -c PowerPolicy --type NM20 --action DisableDomain --domain_id

	<domain ID>
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action DisableDomain --domain_id <domain ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DisableDomain --domain_id 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action DisableDomain --domain_id 0
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DisableDomain --domain_id 0
```

```
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.

#### 5.9.6.1.5. Enabling Specified Node Manager Policy

Use the PowerPolicy command with option --action EnablePolicy to enable specified NM policy of a managed system.

The following are the supported options for option --action EnablePolicy.

Option	Description
--------	-------------

--policy_id	Specifies policy ID from 0 to 255.
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID>
In-Band	saa -c PowerPolicy --type NM20 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action EnablePolicy --domain_id 0 --policy_id 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action EnablePolicy --domain_id 0 --policy_id 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action EnablePolicy --domain_id 0 --policy_id 1
```

```
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.

#### 5.9.6.1.6. Disabling Specified Node Manager Policy

Use the PowerPolicy command with option `--action DisablePolicy` to disable specified NM policy of a managed system.

The following are the supported options for option `--action DisablePolicy`.

Option	Description
<code>--policy_id</code>	Specifies policy ID from 0 to 255.
<code>--domain_id</code>	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type NM20 --action DisablePolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>
In-Band	<code>saa -c PowerPolicy --type NM20 --action DisablePolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>
Multiple Systems	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type NM20 --action DisablePolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DisablePolicy --domain_id 0 --policy_id 1
```

#### In-Band:

---

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action DisablePolicy --
domain_id 0 --policy_id 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
NM20 --action DisablePolicy --domain_id 0 --policy_id 1
```

```
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.

#### 5.9.6.1.7. Adding Power Policy

Use the PowerPolicy command with option --action AddPowerPolicy or AddPolicy to add power policy of a managed system. The following are the supported options for option --action AddPowerPolicy or AddPolicy.

Option	Description
--limit	Specifies policy target limit.
--mode	Specifies aggressive CPU power correction mode. 0: Automatic mode (default) 1: Force non-aggressive mode 2: Force aggressive mode
--period	Specifies statistics reporting period in seconds.
-- exception_action	Specifies policy exception action. 1: Send alert 2: Shutdown system 3: Send alert & Shutdown system
--time	Specifies correction time limit (ms).
--policy_id	Specifies policy ID from 0 to 255.

--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem
--trigger_type	Specifies policy trigger type. 0: No policy trigger 1: Inlet temperature limit policy trigger in [celsius] 2: Missing power reading timeout in 1/10th of second 3: Time after host reset trigger in 1/10th of second 4: Boot time policy 6: MGPIIO policy trigger
--trigger_limit	Specifies policy trigger limit.
--overwrite	Overwrite the policy.

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type NM20 --action AddPowerPolicy --policy_id &lt;policy ID&gt; --limit &lt;limit&gt; --time &lt;time&gt; --period &lt;period&gt; [--overwrite]</pre> <pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type NM20 --action AddPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --trigger_type &lt;trigger type&gt; --mode &lt;mode&gt; -- exception_action &lt;exception action&gt; --limit &lt;limit&gt; --time &lt;time&gt; -- trigger_limit &lt;trigger limit&gt; --period &lt;period&gt; [--overwrite]</pre>
In-Band	<pre>saa -c PowerPolicy --type NM20 --action AddPowerPolicy --policy_id &lt;policy ID&gt; --limit &lt;limit&gt; --time &lt;time&gt; --period &lt;period&gt; [--overwrite]</pre> <pre>saa -c PowerPolicy --type NM20 --action AddPolicy --type NM20 -- action AddPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; -- trigger_type &lt;trigger type&gt; --mode &lt;mode&gt; --exception_action &lt;exception action&gt; --limit &lt;limit&gt; --time &lt;time&gt; --trigger_limit &lt;trigger limit&gt; --period &lt;period&gt; [--overwrite]</pre>
Multiple Systems	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type NM20 --action AddPowerPolicy --policy_id &lt;policy ID&gt; --limit &lt;limit&gt; --time &lt;time&gt; --period &lt;period&gt; [--overwrite]</pre> <pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type NM20 --action AddPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --trigger_type &lt;trigger type&gt; --mode &lt;mode&gt; --</pre>



---

exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> [--overwrite]
-----------------------------------------------------------------------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action AddPowerPolicy --policy_id 1 --limit 200 --time 20000 --period 200 -overwrite
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action AddPolicy --domain_id 0 --policy_id 1 --trigger_type 0 --mode 0 --exception_action 1 --limit 200 --time 20000 --trigger_limit 200 --period 200 -overwrite
```

**In-Band:**

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action AddPowerPolicy --policy_id 1 --limit 200 --time 20000 --period 200 -overwrite
```

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action AddPolicy --domain_id 0 --policy_id 1 --trigger_type 0 --mode 0 --exception_action 1 --limit 200 --time 20000 --trigger_limit 200 --period 200 -overwrite
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action AddPowerPolicy --policy_id 1 --limit 200 --time 20000 --period 200 -overwrite
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action AddPolicy --domain_id 0 --policy_id 1 --trigger_type 0 --mode 0 --exception_action 1 --limit 200 --time 20000 --trigger_limit 200 --period 200 -overwrite
```

```
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.

#### 5.9.6.1.8. Getting Policy

Use the PowerPolicy command with option --action GetPolicy to get policy from a managed system.

The following are the supported options for option --action GetPolicy.

Option	Description
--policy_id	Specifies policy ID from 0 to 255.
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID>
In-Band	saa -c PowerPolicy --type NM20 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action GetPolicy --domain_id 0 --policy_id 1
```

#### In-Band:

---

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action GetPolicy --
domain_id 0 --policy_id 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
NM20 --action GetPolicy --domain_id 0 --policy_id 1
```

```
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.

#### 5.9.6.1.9. Deleting Policy

Use the PowerPolicy command with option --action DelPolicy to delete policy of a managed system.

The following are the supported options for option --action DelPolicy.

Option	Description
--policy_id	Specifies policy ID from 0 to 255.
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID>
In-Band	saa -c PowerPolicy --type NM20 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID>
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID>
-----	-------------------------------------------------------------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DelPolicy --domain_id 0 --policy_id 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action DelPolicy --domain_id 0 --policy_id 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DelPolicy --domain_id 0 --policy_id 1
```

```
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.

#### 5.9.6.1.10. Scanning Policy

Use the PowerPolicy command with option --action ScanPolicy to scan all presented policies of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action ScanPolicy
In-Band	saa -c PowerPolicy --type NM20 --action ScanPolicy
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action ScanPolicy
-----	--------------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action ScanPolicy
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action ScanPolicy
```

The console output contains the following information.

```
=====
Domain ID = 0 , Policy ID = 3
=====
Values:
Power Limit = 200 w
Correction Time limit = 20000 ms
Statistics Reporting Period = 200 s
Policy Trigger Limit = 200
Domain ID:
 Entire platform
Policy state:
 Policy(Enabled) Domain(Enabled) Global(Enabled)
Policy Trigger Type:
 No Policy Trigger
Aggressive CPU Power correction:
 Backward compatible with NMV1.5
Policy Exception action state:
 Send alert
raw = 57 01 00 70 10 01 C8 00 20 4E 00 00 C8 00 C8 00

Alert Thresholds:
Number of alert thresholds = 0

Suspend Periods:
Number Of Periods = 0

Total Policies = 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action ScanPolicy
```

```
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.

#### 5.9.6.1.11. Getting Policy Alert Thresholds

Use the PowerPolicy command with option `--action GetAlertThreshold` to get policy alert thresholds from a managed system.

The following are the supported options for option `--action GetAlertThreshold`.

Option	Description
<code>--policy_id</code>	Specifies policy ID from 0 to 255.
<code>--domain_id</code>	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type NM20 --action GetAlertThreshold --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>
In-Band	<code>saa -c PowerPolicy --type NM20 --action GetAlertThreshold --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>
Multiple Systems	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type NM20 --action GetAlertThreshold --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type NM20 --action GetAlertThreshold --domain_id 0 --policy_id 1
```

**In-Band:**

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action GetAlertThreshold -
-domain_id 0 --policy_id 1
```

**The console output contains the following information.**

```
Number of alert thresholds = 3
Threshold[0] = 150
Threshold[1] = 250
Threshold[2] = 300
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
NM20 --action GetAlertThreshold --domain_id 0 --policy_id 1
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

Use the PowerPolicy command with option --action SetAlertThreshold to set policy alert thresholds of a managed system. The following are the supported options for option --action SetAlertThreshold.

#### 5.9.6.1.12. Setting Policy Alert Thresholds

Use the PowerPolicy command with option --action GetAlertThreshold to get policy alert thresholds from a managed system.

The following are the supported options for option --action GetAlertThreshold.

Option	Description
--policy_id	Specifies policy ID from 0 to 255.
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem
--value	Specifies threshold value. Up to three threshold values, and each threshold is separated by commas (,).
--count	Specifies count. 0 : Clear all thresholds [1-3] : Number of alert thresholds

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action SetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> --count <count> --value <value>
In-Band	saa -c PowerPolicy --type NM20 --action SetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> --count <count> --value <value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action SetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> --count <count> --value <value>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type NM20 --action SetAlertThreshold --domain_id 0 --policy_id 1 --count
3 --value 100,200,300
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action SetAlertThreshold -
-domain_id 0 --policy_id 1 --count 3 --value 100,200,300
```



## Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action SetAlertThreshold --domain_id 0 --policy_id 1 --count 3 --value 100,200,300
```

```
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.

### 5.9.6.1.13. Getting Suspension Period

Use the PowerPolicy command with option --action GetPeriod to get suspension period from managed system.

The following are the supported options for option --action GetPeriod.

Option	Description
--policy_id	Specifies policy ID from 0 to 255.
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action GetPeriod --domain_id <domain ID> --policy_id <policy ID>
In-Band	saa -c PowerPolicy --type NM20 --action GetPeriod --domain_id <domain ID> --policy_id <policy ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action GetPeriod --domain_id <domain ID>

---

	<code>--policy_id &lt;policy ID&gt;</code>
--	--------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type NM20 --action GetPeriod --domain_id 0 --policy_id 0
```

**In-Band:**

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action GetPeriod --
domain_id 0 --policy_id 0
```

**The console output contains the following information.**

```
Number Of Periods = 1
[Suspend Periods 1]
 Start = 00:00
 Stop = 23:54
 Days = Monday Tuesday Wednesday
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
NM20 --action GetPeriod --domain_id 0 --policy_id 0
```

```
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.

#### 5.9.6.1.14. Adding Suspension Period

Use the PowerPolicy command with option `--action AddPeriod` to add suspension period from managed system.

The following are the supported options for option `--action AddPeriod`.

Option	Description
--policy_id	Specifies policy ID from 0 to 255.
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem
--st	Policy suspension start time (HHmm) [0000-2359]
--et	Policy suspension end time (HHmm) [0006-2400] If there is a need to specify an end-time that is beyond midnight Two suspension periods.
--days	Suspend period recurrence 1 – Monday, 2 – Tuesday, 3 – Wednesday, 4 – Thursday, 5 – Friday, 6 – Saturday, 7 - Sunday

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action AddPeriod --domain_id <domain ID> --policy_id <policy ID> --st <start time> --et <end time> --days <Days>
In-Band	saa -c PowerPolicy --type NM20 --action AddPeriod --domain_id <domain ID> --policy_id <policy ID> --st <start time> --et <end time> -- days <Days>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action AddPeriod --domain_id <domain ID> --policy_id <policy ID> --st <start time> --et <end time> --days <Days>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type NM20 --action AddPeriod --domain_id 0 --policy_id 0 --st 0000 --et
0006 --days 123
```

#### In-Band:

---

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action AddPeriod --
domain_id 0 --policy_id 0 --st 0000 --et 0006 --days 123
```

**The console output contains the following information.**

```
Done
=====
```

Domain ID = 0 , Policy ID = 0

```
=====
```

#### **Multiple 00B:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
NM20 --action AddPeriod --domain_id 0 --policy_id 0 --st 0000 --et 0006 -
-days 123
```

```
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.

#### **5.9.6.1.15. Updating Suspension Period**

Use the PowerPolicy command with option `--action UpdatePeriod` to update suspension period from managed system.

The following are the supported options for option `--action UpdatePeriod`.

Option	Description
<code>--policy_id</code>	Specifies policy ID from 0 to 255.
<code>--domain_id</code>	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem

--period_id	Period ID 1~5 for which policy should be used
--st	Policy suspension start time (HHmm) [0000-2359]
--et	Policy suspension end time (HHmm) [0006-2400] If there is a need to specify an end-time that is beyond midnight Two suspension periods.
--days	Suspend period recurrence 1 – Monday, 2 – Tuesday, 3 – Wednesday, 4 – Thursday, 5 – Friday, 6 – Saturday, 7 - Sunday

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action UpdatePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID> --st <start time> --et <end time> --days <Days>
In-Band	saa -c PowerPolicy --type NM20 --action UpdatePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID> --st <start time> --et <end time> --days <Days>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action UpdatePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID> --st <start time> --et <end time> --days <Days>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type NM20 --action UpdatePeriod --domain_id 0 --policy_id 0 --period_id 1
--st 0000 --et 0006 --days 123
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action UpdatePeriod --
domain_id 0 --policy_id 0 --period_id 1 --st 0000 --et 0006 --days 123
```

The console output contains the following information.

```

Done
=====
Domain ID = 0 , Policy ID = 0
=====

```

### Multiple OOB:

```

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
NM20 --action UpdatePeriod --domain_id 0 --policy_id 0 --period_id 1 --st
0000 --et 0006 --days 123

```

```

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.

#### 5.9.6.1.16. Deleting Suspension Period

Use the PowerPolicy command with option `--action DeletePeriod` to delete suspension period from managed system.

The following are the supported options for option `--action DeletePeriod`.

Option	Description
<code>--policy_id</code>	Specifies policy ID from 0 to 255.
<code>--domain_id</code>	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem
<code>--period_id</code>	Period ID 1~5 for which policy should be used

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type NM20 --action DeletePeriod --domain_id &lt;domain</code>

	ID> --policy_id <policy ID> --period_id <Period ID>
In-Band	saa -c PowerPolicy --type NM20 --action DeletePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID>
<b>Multiple Systems</b>	
OoB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action DeletePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID>

Example:

#### OoB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DeletePeriod --domain_id 0 --policy_id 0 --period_id 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action DeletePeriod --domain_id 0 --policy_id 0 --period_id 1
```

The console output contains the following information.

```
Done
=====
Domain ID = 0 , Policy ID = 0
=====
```

#### Multiple OoB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action DeletePeriod --domain_id 0 --policy_id 0 --period_id 1
```

```
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.

---

### 5.9.6.1.17. Clearing Suspension Period

Use the PowerPolicy command with option `--action ClearPeriod` to clear suspension period from managed system.

The following are the supported options for option `--action ClearPeriod`.

Option	Description
<code>--policy_id</code>	Specifies policy ID from 0 to 255.
<code>--domain_id</code>	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem
<code>--period_id</code>	Period ID 1~5 for which policy should be used

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type NM20 --action ClearPeriod --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --period_id &lt;Period ID&gt;</code>
In-Band	<code>saa -c PowerPolicy --type NM20 --action ClearPeriod --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --period_id &lt;Period ID&gt;</code>
Multiple Systems	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type NM20 --action ClearPeriod --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --period_id &lt;Period ID&gt;</code>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action ClearPeriod --domain_id 0 --policy_id 0 --period_id 1
```

**In-Band:**



```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action ClearPeriod --domain_id 0 --policy_id 0 -period_id 1
```

The console output contains the following information.

```
Done
=====
Domain ID = 0 , Policy ID = 0
=====
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type NM20 --action ClearPeriod --domain_id 0 --policy_id 0 -period_id 1
```

```
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.

### 5.9.6.2. Managing the Power Policy by BMC Intel Node Manager

When managing the power policy by the BMC Intel Node Manager, some domain management requires Power into System (Psys) support. For the usage of the PowerPolicy command with the --type BMC10 (BMC Intel Node Manager 1.0) option, the --domain\_id option with 0 (Entire platform, AC power), 4 (PCIe devices subsystem) or 5 (Entire platform, DC power) requires Psys support.

#### 5.9.6.2.1 Enabling BMC Intel Node Manager Policy Control Globally

Use the PowerPolicy command with --action EnableGlobal option to globally enable BMC Intel Node Manager policy control for a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action EnableGlobal

In-Band	saa -c PowerPolicy --type BMC10 --action EnableGlobal
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action EnableGlobal

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action EnableGlobal
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action EnableGlobal
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action EnableGlobal
```

```
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 created log file.

#### 5.9.6.2.2. Disabling BMC Intel Node Manager Policy Control Globally

Use the PowerPolicy command with the --action DisableGlobal option to globally disable BMC Intel Node Manager policy control for a managed system.

<b>Single System</b>	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action DisableGlobal
In-Band	saa -c PowerPolicy --type BMC10 --action DisableGlobal

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action DisableGlobal

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action DisableGlobal
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action DisableGlobal
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action DisableGlobal
```

```
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 created log file.

#### 5.9.6.2.3. Enabling BMC Intel Node Manager Policies for the Specified Domain

Use the PowerPolicy command with the --action EnableDomain option to enable BMC Intel Node Manager policies for the specified domain of a managed system.

The following option is supported for the --action EnableDomain option.

Option	Description
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem

	4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)
--	-----------------------------------------------------------------------------------------------------------------

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action EnableDomain --domain_id <domain ID>
In-Band	saa -c PowerPolicy --type BMC10 --action EnableDomain --domain_id <domain ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action EnableDomain --domain_id <domain ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action EnableDomain --domain_id 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action EnableDomain --domain_id 0
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action EnableDomain --domain_id 0
```

```
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 created log file.

---

#### 5.9.6.2.4. Disabling BMC Intel Node Manager Policies for the Specified Domain

Use the PowerPolicy command with option --action DisableDomain to disable BMC Intel Node Manager policies for specified domain of a managed system.

The following is the supported option for option --action DisableDomain.

Option	Description
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action DisableDomain --domain_id <domain ID>
In-Band	saa -c PowerPolicy --type BMC10 --action DisableDomain --domain_id <domain ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action DisableDomain --domain_id <domain ID>

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action DisableDomain --domain_id 0
```

##### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action DisableDomain --domain_id 0
```

##### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action DisableDomain --domain_id 0
```

```
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 created log file.

#### 5.9.6.2.5. Enabling the Specified BMC Intel Node Manager Policy

Use the PowerPolicy command with the --action EnablePolicy option to enable the specified BMC Intel Node Manager policy of a managed system.

The following options for are supported for the --action EnablePolicy option.

Option	Description
--policy_id	Specifies a policy ID from 0 to 255.
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID>
In-Band	saa -c PowerPolicy --type BMC10 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID>

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type BMC10 --action EnablePolicy --domain_id 0 --policy_id 1
```

**In-Band:**

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action EnablePolicy --
domain_id 0 --policy_id 1
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
BMC10 --action EnablePolicy --domain_id 0 --policy_id 1
```

```
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 created log file.

#### 5.9.6.2.6. Disabling the Specified BMC Intel Node Manager Policy

Use the PowerPolicy command with the --action DisablePolicy option to disable the specified BMC Intel Node Manager policy of a managed system.

The following options are supported for the --action DisablePolicy option.

Option	Description
--policy_id	Specifies a policy ID from 0 to 255.
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID>
In-Band	saa -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id 0 --policy_id 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id 0 --policy_id 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id 0 --policy_id 1
```

```
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 created log file.

#### 5.9.6.2.7. Adding Power Policy



Use the PowerPolicy command with option --action AddPowerPolicy or AddPolicy to add power policy of a managed system. The following are the supported options for option --action AddPowerPolicy or AddPolicy.

Option	Description
--limit	<p>For AddPowerPolicy action: Specifies policy target limit (watts) from 0 to 32767.</p> <p>For AddPolicy action: Specifies policy target limit. For policy trigger type 0, 1, 3, 6, 7 and 8: [0-32767] watts For policy trigger type 2: [0-100] percentage Not required for policy trigger type 9.</p>
--mode	<p>Specifies aggressive CPU power correction mode.</p> <p>0: Automatic mode (default) 1: Force non-aggressive mode 2: Force aggressive mode</p>
--period	Specifies statistics reporting period in seconds from 1 to 3600.
--exception_action	<p>Specifies the policy exception action.</p> <p>1: Sends alert 2: Shutdowns system 3: Sends alert and shutdowns system</p>
--time	Specifies correction time limit (ms) from 1000 to 60000.
--policy_id	Specifies policy ID from 0 to 255.
--domain_id	<p>0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)</p>
--trigger_type	<p>Specifies policy trigger type.</p> <p>0: No policy trigger 1: Inlet temperature limit policy trigger in [celsius] 2: Missing power reading timeout in 1/10th of second 3: Time after host reset trigger in 1/10th of second</p>

	6: MGPIO policy trigger 7: C0 Residency in [%] 8: Host Reset 9: SMBAlert Interrupt
--trigger_limit	Specifies policy trigger limit for policy trigger type 1-3 and 7. Otherwise, set to 0. For policy trigger type 1 : [0-100] degrees C For policy trigger type 2, 3: [1-32760], divided by 10 to seconds. For policy trigger type 7: [0-100] percentage
--storage	Specifies storage option. 1: Volatile memory
--overwrite	Overwrite the policy.

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type BMC10 --action AddPowerPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --limit &lt;limit&gt; --time &lt;time&gt; -- period &lt;period&gt; --storage &lt;storage&gt; [--overwrite]</pre> <pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type BMC10 --action AddPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --trigger_type &lt;trigger type&gt; --mode &lt;mode&gt; --exception_action &lt;exception action&gt; --limit &lt;limit&gt; --time &lt;time&gt; --trigger_limit &lt;trigger limit&gt; --period &lt;period&gt; --storage &lt;storage&gt; [--overwrite]</pre>
In-Band	<pre>saa -c PowerPolicy --type BMC10 --action AddPowerPolicy -- domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --limit &lt;limit&gt; --time &lt;time&gt; --period &lt;period&gt; --storage &lt;storage&gt; [--overwrite]</pre> <pre>saa -c PowerPolicy --type BMC10 --action AddPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --trigger_type &lt;trigger type&gt; -- mode &lt;mode&gt; --exception_action &lt;exception action&gt; --limit &lt;limit&gt; -- time &lt;time&gt; --trigger_limit &lt;trigger limit&gt; --period &lt;period&gt; --storage &lt;storage&gt; [--overwrite]</pre>
Multiple Systems	

OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type BMC10 --action AddPowerPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --limit &lt;limit&gt; --time &lt;time&gt; -- period &lt;period&gt; --storage &lt;storage&gt; [--overwrite]  saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type BMC10 --action AddPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt; --trigger_type &lt;trigger type&gt; --mode &lt;mode&gt; --exception_action &lt;exception action&gt; --limit &lt;limit&gt; --time &lt;time&gt; --trigger_limit &lt;trigger limit&gt; --period &lt;period&gt; --storage &lt;storage&gt; [--overwrite]</pre>
-----	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type BMC10 --action AddPowerPolicy --domain_id 0 --policy_id 1 --limit
200 --time 20000 --period 200 --storage 1 --overwrite
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type BMC10 --action AddPolicy --domain_id 0 --policy_id 1 --trigger_type
0 --mode 0 --exception_action 1 --limit 200 --time 20000 --trigger_limit
200 --period 200 --storage 1 --overwrite
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action AddPowerPolicy --
domain_id 0 --policy_id 1 --limit 200 --time 20000 --period 200 --storage
1 --overwrite
```

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action AddPolicy --
domain_id 0 --policy_id 1 --trigger_type 0 --mode 0 --exception_action 1
--limit 200 --time 20000 --trigger_limit 200 --period 200 --storage 1 --
overwrite
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
BMC10 --action AddPowerPolicy --domain_id 0 --policy_id 1 --limit 200 --
time 20000 --period 200 --storage 1 --overwrite
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
BMC10 --action AddPolicy --domain_id 0 --policy_id 1 --trigger_type 0 --
mode 0 --exception_action 1 --limit 200 --time 20000 --trigger_limit 200
--period 200 --storage 1 --overwrite
```

```
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.

### 5.9.6.2.8. Getting Policy

Use the PowerPolicy command with option `--action GetPolicy` to get policy from a managed system.

The following are the supported options for option `--action GetPolicy`.

Option	Description
<code>--policy_id</code>	Specifies policy ID from 0 to 255.
<code>--domain_id</code>	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type BMC10 --action GetPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>
In-Band	<code>saa -c PowerPolicy --type BMC10 --action GetPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>
Multiple Systems	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type BMC10 --action GetPolicy --domain_id &lt;domain</code>

---

ID> --policy_id <policy ID>
-----------------------------

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type BMC10 --action GetPolicy --domain_id 1 --policy_id 60
```

**The console output contains the following information.**

```
Values:
Power Limit = 210 w
Correction Time limit = 6000 ms
Statistics Reporting Period = 10 s
Policy Trigger Limit = 210
Domain ID:
 CPU subsystem
Policy state:
 Policy(Enabled) Domain(Enabled) Global(Disabled)
Policy Trigger Type:
 No Policy Trigger
Aggressive CPU Power correction:
 Backward compatible with NMV1.5
Policy Exception action state:
 Send alert
raw = 57 01 00 31 90 01 D2 00 70 17 00 00 D2 00 0A 0
```

**In-Band:**

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action GetPolicy --
domain_id 1 --policy_id 60
```

**Multiple OoB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
BMC10 --action GetPolicy --domain_id 1 --policy_id 60
```

```
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.

#### 5.9.6.2.9. Deleting Policy

Use the PowerPolicy command with option `--action DelPolicy` to delete policy of a managed system.

The following are the supported options for option `--action DelPolicy`.

Option	Description
<code>--policy_id</code>	Specifies policy ID from 0 to 255.
<code>--domain_id</code>	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c PowerPolicy --type BMC10 --action DelPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>
In-Band	<code>saa -c PowerPolicy --type BMC10 --action DelPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>
Multiple Systems	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c PowerPolicy --type BMC10 --action DelPolicy --domain_id &lt;domain ID&gt; --policy_id &lt;policy ID&gt;</code>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action DelPolicy --domain_id 0 --policy_id 1
```

**In-Band:**

---

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action DelPolicy --domain_id 0 --policy_id 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action DelPolicy --domain_id 0 --policy_id 1
```

```
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.

#### 5.9.6.2.10. Scanning Policy

Use the PowerPolicy command with option --action ScanPolicy to scan all presented policies of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action ScanPolicy
In-Band	saa -c PowerPolicy --type BMC10 --action ScanPolicy
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action ScanPolicy

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action ScanPolicy
```

The console output contains the following information.

```

=====
Domain ID = 1 , Policy ID = 60
=====
Values:
Power Limit = 210 w
Correction Time limit = 6000 ms
Statistics Reporting Period = 10 s
Policy Trigger Limit = 210
Domain ID:
 CPU subsystem
Policy state:
 Policy(Enabled) Domain(Enabled) Global(Disabled)
Policy Trigger Type:
 No Policy Trigger
Aggressive CPU Power correction:
 Backward compatible with NMV1.5
Policy Exception action state:
 Send alert
raw = 57 01 00 31 90 01 D2 00 70 17 00 00 D2 00 0A 00

Total Policies = 1

```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action ScanPolicy
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
BMC10 --action ScanPolicy
```

```

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.

#### **5.9.6.2.11. Getting Limiting Policy ID**

Use the PowerPolicy command with the --action GetLimitPolicyId option to get limiting policy ID of a managed system.



Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action GetLimitPolicyId
In-Band	saa -c PowerPolicy --type BMC10 --action GetLimitPolicyId
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action GetLimitPolicyId

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action GetLimitPolicyId
```

The console output contains the following information.

```
Current limiting policy ID = 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action GetLimitPolicyId
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type BMC10 --action GetLimitPolicyId
```

```
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.

## 5.9.7. Managing Data Center Manageability Interface

---

The DcmiManage command can manage the system through the Data Center Manageability Interface (DCMI) for Supermicro platforms.

The following table summarizes the supported actions in the DcmiManage command with the standard DCMI specification and Intel Node Manager version 2.0.

Option	--type	--action
Description	STD_DCMI = Standard DCMI specification	Find = Finds DCMI device from local or IP range GetCap = Lists DCMI capabilities information GetPowerStatus = Displays DCMI power reading information GetMCID = Lists management controller identifier string SetMCID = Sets management controller identifier string
	NM20 = Node manager 2.0	GetCap = Gets DCMI capability information GetPowerReading = Gets power reading GetPowerLimit = Gets power limit SetPowerLimit = Sets power limit EnablePowerLimit = Enables power limit DisablePowerLimit = Disables power limit



**Note:** Starting with the 14th generation Intel platform, the --type STD\_DCMI and NM20 options are not supported since these platforms lack Management Engine (ME) required for Intel Node Manager management.

---

### 5.9.7.1. Standard Data Center Manageability Interface Specification

#### 5.9.7.1.1. Finding Data Center Manageability Interface Device from Local or IP Range

Use the DcmiManage command with option --action Find to search for and display all DCMI devices of managed system.

The following are the supported options for option --action Find.

Option	Description
--------	-------------

--start_ip	Specifies IPv4 IP address.
--end_ip	Specifies IPv4 IP address.
--netmask	Specifies netmask.

Single System	
In-Band	saa -c DcmiManage --type STD_DCMI --action Find [--start_ip <start IP> --end_ip <end IP> --netmask <netmask>]

Example:

#### In - Band :

```
[SAA_HOME]# ./saa -c DcmiManage --type STD_DCMI --action Find --start_ip
192.168.34.1 --end_ip 192.168.34.100 --netmask 255.255.255.0
```

The console output contains the following information.

```
Finding DCMI Devices
192.168.34.1 DCMI Ver:1.1
192.168.34.2 DCMI Ver:1.1
192.168.34.3 DCMI Ver:1.1
3 DCMI device(s) found
```

#### 5.9.7.1.2. Listing Data Center Manageability Interface Capabilities Information

Use the DcmiManage command with option --action GetCap to list the DCMI capabilities of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type STD_DCMI --action GetCap
In-Band	saa -c DcmiManage --type STD_DCMI --action GetCap
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c

---

DcmiManage --type STD_DCMI --action GetCap
--------------------------------------------

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --
type STD_DCMI --action GetCap
```

**In-Band:**

```
[SAA_HOME]# ./saa -c DcmiManage --type STD_DCMI --action GetCap
```

**The console output contains the following information.**

```
DCMI Version = 1.1
Mandatory Platform capabilities
Temperature Monitor :Compliant
Chassis Power :Compliant
SEL logging :Compliant
Identification Support :Compliant

Optional Platform capabilities
Power Management :Compliant

Manageability Access Capabilities
VLAN Capable :Available
SOL Supported :Available
OoB Primary LAN Channel Available :Available
OoB Secondary LAN Channel Available :Not present
OoB Serial TMODE Available :Not present
In-Band KCS Channel Available :Available

SEL Attributes
SEL automatic rollover enabled :Not present
Number of SEL entries :0

Identification Attributes
Asset Tag Support :Available
DHCP Host Name Support :Not present
GUID Support :Available

Temperature Monitoring
Baseboard temperature :At least 1
Processors temperature :At least 1
Inlet temperature :At least 1

Power Management Device Slave Address
```

```

7-bit I2C Slave Address of device on IPMB :10

Power Management Controller Channel Number
Channel Number :00
Device Revision :01

Manageability Access Attributes
Mandatory Primary LAN OOB Support(RMCP+ Support Only) :supported
Optional Secondary LAN OOB Support(RMCP+ Support Only):Not supported
Optional Serial OOB TMODE Capability :Not supported

```

## Multiple OOB:

```

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type
STD_DCMI --action GetCap

```

```

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.

### 5.9.7.1.3. Displaying Data Center Manageability Interface Power Reading Information

Use the DcmiManage command with option --action GetPowerStatus to display the related DCMI power status of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type STD_DCMI --action GetPowerStatus
In-Band	saa -c DcmiManage --type STD_DCMI --action GetPowerStatus
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action GetPowerStatus

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --
type STD_DCMI --action GetPowerStatus
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c DcmiManage --type STD_DCMI --action GetPowerStatus
```

**The console output contains the following information.**

```
Instantaneous power reading | 121 W
Minimum during sampling period | 65 W
Maximum during sampling period | 482 W
Average during sampling period | 123 W
IPMI timestamp | 2023/08/28 07:29:10
Sampling period | 115418000 Milliseconds
Power reading state | Activated
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type
STD_DCMI --action GetPowerStatus
```

```
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.

#### **5.9.7.1.4. Getting Management Controller Identifier String**

Use the DcmiManage command with option --action GetMCID to get the management controller identifier string from a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type STD_DCMI --action GetMCID
In-Band	saa -c DcmiManage --type STD_DCMI --action GetMCID

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action GetMCID

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type STD_DCMI --action GetMCID
```

#### In-Band:

```
[SAA_HOME]# ./saa -c DcmiManage --type STD_DCMI --action GetMCID
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type STD_DCMI --action GetMCID
```

```
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.

#### 5.9.7.1.5. Setting Management Controller Identifier String

Use the DcmiManage command with option --action SetMCID to set the management controller identifier string from a managed system.

The following is the supported option for option --action SetMCID.

Option	Description
--value	Specifies MCID string value.

Single System
---------------

OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type STD_DCMI --action SetMCID --value <value>
In-Band	saa -c DcmiManage --type STD_DCMI --action SetMCID --value <value>
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action SetMCID --value <value>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type STD_DCMI --action SetMCID --value example
```

**In-Band:**

```
[SAA_HOME]# ./saa -c DcmiManage --type STD_DCMI --action SetMCID --value example
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type STD_DCMI --action SetMCID --value example
```

```
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.

## 5.9.7.2. Intel Intelligent Power Node Manager V2.0

### 5.9.7.2.1. Getting Data Center Manageability Interface Capability Information

Use the DcmiManage command with option --action GetCap to get DCMI capability information from a managed system.



Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type NM20 --action GetCap
In-Band	saa -c DcmiManage --type NM20 --action GetCap
Multiple Systems	
OOB	saa -l< system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action GetCap

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action GetCap
```

#### In-Band:

```
[SAA_HOME]# ./saa -c DcmiManage --type NM20 --action GetCap
```

**The console output contains the following information.**

```
Enhanced Power Statistics attributes
DCMI Version :1.1
Parameter Revision:2
The number of supported rolling average time periods:9
Rolling Average Time periods:
 05 - 5 Seconds
 0F - 15 Seconds
 1E - 30 Seconds
 41 - 1 Minutes
 43 - 3 Minutes
 47 - 7 Minutes
 4F - 15 Minutes
 5E - 30 Minutes
 81 - 1 Hours
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action GetCap
```

```
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.

#### 5.9.7.2.2. Getting Power Reading

Use the DcmiManage command with option --action GetPowerReading to get power reading from a managed system.

The following are the supported option for option --action GetPowerReading.

Option	Description
--mode	Specifies power reading mode. 1: System Power Statistics 2: Enhanced System Power Statistics
--period	Specifies rolling average time period. Please execute DcmiManage command with --type NM20 and --action GetCap to get supported period(hex value).

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type NM20 --action GetPowerReading --mode <mode> [--period <period>]
In-Band	saa -c DcmiManage --type NM20 --action GetPowerReading --mode <mode> [--period <period>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action GetPowerReading --mode <mode> [--period <period>]

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action GetPowerReading -mode 2 --period 05
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c DcmiManage --type NM20 --action GetPowerReading -mode 2 --period 05
```

**The console output contains the following information.**

```
Instantaneous power reading | 107 W
Minimum during sampling period | 77 W
Maximum during sampling period | 207 W
Average during sampling period | 126 W
IPMI timestamp | 2023/08/28 07:54:00
Sampling period | 5 Seconds
Power reading state | Activated
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action GetPowerReading -mode 2 --period 05
```

```
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.

#### **5.9.7.2.3. Getting Power Limit**

Use the DcmiManage command with option --action GetPowerLimit to get power limit from a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type NM20 --action GetPowerLimit

In-Band	saa -c DcmiManage --type NM20 --action GetPowerLimit
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action GetPowerLimit

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action GetPowerLimit
```

#### In-Band:

```
[SAA_HOME]# ./saa -c DcmiManage --type NM20 --action GetPowerLimit
```

The console output contains the following information.

```
Exception actions :Hard power off system and log event to SEL
Power limit requested :200 W
Correction time limit :20000 ms
Management application statistics sampling period :50 s
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action GetPowerLimit
```

```
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.

#### 5.9.7.2.4. Setting Power Limit

Use the DcmiManage command with option --action SetPowerLimit to set power limit from a managed system.

The following are the supported options for option --action SetPowerLimit.

Option	Description
--limit	Specifies power limit in watts.
--period	Specifies management application statistics sampling period in seconds.
--exception_action	Specifies exception action. 0: No Action 1: Hard power off system and log event to SEL 17: Log event to SEL
--time	Specifies correction time limit in milliseconds.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type NM20 --action SetPowerLimit --exception_action <exception action> --limit <limit> --time <time> --period <period>
In-Band	saa -c DcmiManage --type NM20 --action SetPowerLimit --exception_action <exception action> --limit <limit> --time <time> --period <period>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action SetPowerLimit --exception_action <exception action> --limit <limit> --time <time> --period <period>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action SetPowerLimit --exception_action 1 --limit 200 --time 20000 --period 50
```

**In-Band:**

```
[SAA_HOME]# ./saa -c DcmiManage --type NM20 --action SetPowerLimit --exception_action 1 --limit 200 --time 20000 --period 50
```

The console output contains the following information.

```
Exception actions :Hard power off system and log event to SEL
Power limit requested :200 W
Correction time limit :20000 ms
Management application statistics sampling period :50 s
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action SetPowerLimit --exception_action 1 --limit 200 --time 20000 --period 50
```

```
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.

#### 5.9.7.2.5. Enabling Power Limit

Use the DcmiManage command with option --action EnablePowerLimit to enable the power limit from a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type NM20 --action EnablePowerLimit
In-Band	saa -c DcmiManage --type NM20 --action EnablePowerLimit
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action EnablePowerLimit

Example:

---

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action EnablePowerLimit
```

**In-Band:**

```
[SAA_HOME]# ./saa -c DcmiManage --type NM20 --action EnablePowerLimit
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type NM20 --action EnablePowerLimit
```

```
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.

#### 5.9.7.2.6. Disabling Power Limit

Use the DcmiManage command with option --action DisablePowerLimit to enable the power limit from a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type NM20 --action DisablePowerLimit
In-Band	saa -c DcmiManage --type NM20 --action DisablePowerLimit
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action DisablePowerLimit

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --
type NM20 --action DisablePowerLimit
```

**In-Band:**

```
[SAA_HOME]# ./saa -c DcmiManage --type NM20 --action DisablePowerLimit
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type
NM20 --action DisablePowerLimit
```

```
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.

### 5.9.8. Getting AIOM Standby Power Configuration of the Managed System

Use the “GetAiomStandbyPower” command to retrieve AIOM Standby Power configuration information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetAiomStandbyPower
In-Band	saa -l Redfish_HI -u <username> -p <password> -c GetAiomStandbyPower
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetAiomStandbyPower

Example:

**OOB:**



---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetAiomStandbyPower
```

**The console output contains the following information.**

```
Managed
system.....192.168.34.56
AIOM NIC Power in S5 State (Shutdown)On
```

#### **In-Band Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
GetAiomStandbyPower
```

**The console output contains the following information.**

```
Managed
system.....192.168.34.56
AIOM NIC Power in S5 State (Shutdown)On
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetAiomStandbyPower
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### **5.9.9. Setting AIOM Standby Power Configuration of the Managed System**

Use the “SetAiomStandbyPower” command to configure the AIOM Standby Power settings for the managed system. This command provides "On/Off" options to control the AIOM network card and Standby Fan(s), with the default setting being "On."

<b>Single System</b>
----------------------

OOB	saa -i <IP or host name> -u <username> -p <password> -c SetAiomStandbyPower --action <action>
In-Band	saa -I Redfish_HI -u <username> -p <password> -c SetAiomStandbyPower --action <action>
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SetAiomStandbyPower --action <action>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SetAiomStandbyPower --action On
```

The console output contains the following information.

```
Proceeding to AIOM Standby Power On the managed system.
Managed
system.....192.168.34.56
AIOM NIC Power in S5 State (Shutdown)On
```

#### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
SetAiomStandbyPower --action Off
```

The console output contains the following information.

```
Proceeding to AIOM Standby Power Off the managed system.
Managed
system.....192.168.34.56
AIOM NIC Power in S5 State (Shutdown)Off
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
SetAiomStandbyPower --action Off
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### 5.9.10. Getting PSFRU (Power Supply Field Replaceable Unit) Information

Use the “GetPsFruInfo” command to get the current PSFRU (Power Supply Field Replaceable Unit) information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetPsFruInfo
In-Band	saa -c GetPsFruInfo
Multiple Systems	
OOB	saa -l <system list file> -u <username> -p <password> -c GetPsFruInfo

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetPsFruInfo
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GetPsFruInfo
```

The console output contains the following information.

```
[Module 1](SlaveAddress = 0x70)
Status: On
Temperature: 60
Fan 1: 6688 RPM
Fan 2: N/A
```

#### Multiple Systems OOB:

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetPsFruInfo
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

## 5.10. PCIe-Switch Management

### 5.10.1. Getting PCIeSwitch Information

Use the “GetPCleSwitchInfo” command to get and read the PCIe Switch information of the managed system and parse PCIe Switch information from the firmware file.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetPCleSwitchInfo
In-Band	saa -c GetPCleSwitchInfo [--file <filename> [--file_only]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetPCleSwitchInfo

Example:

**In - Band :**

```
[SAA_HOME]# ./saa -c GetPCleSwitchInfo
```

```
[SAA_HOME]# ./saa -c GetPCleSwitchInfo --file fw_file.img --file_only
```

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetPCIESwitchInfo
```

**The console output contains the following information** for the Broadcom chipset on the H12DGQ-NT6 system.

```
Managed system.....localhost
PCIe Switch Device Vendor.....Broadcom
 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.....d9bd7434

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
```

---

**The console output contains the following information** for the Broadcom chipset on the X13DEG-PVC system.

```
Managed system.....localhost
 Device ID(0)
 Device Name.....SwitchPlx0
 Chip Vendor.....Broadcom
 Work Mode.....Base Mode
 Generation.....5
 Subsystem ID.....0072
 SBR version.....00161176

 Device ID(1)
 Device Name.....SwitchPlx1
 Chip Vendor.....Broadcom
 Work Mode.....Base Mode
 Generation.....5
 Subsystem ID.....0072
 SBR version.....00173F18

 Device ID(2)
 Device Name.....SwitchPlx2
 Chip Vendor.....Broadcom
 Work Mode.....Synthetic Mode
 Generation.....5
 FW version.....04:11:00:00
 SBR version.....00:23:24:82
 MfgRevision.....00:23:24:82
 Platform Name.....AOM-SXM5-IO

 Device ID(3)
 Device Name.....SwitchPlx3
 Chip Vendor.....Broadcom
 Work Mode.....Synthetic Mode
 Generation.....5
 FW version.....04:11:00:00
 SBR version.....00:23:24:82
 MfgRevision.....00:23:24:82
 Platform Name.....AOM-SXM5-IO

 Device ID(4)
 Device Name.....SwitchPlx4
 Chip Vendor.....Broadcom
 Work Mode.....Synthetic Mode
 Generation.....5
 FW version.....04:11:00:00
 SBR version.....00:23:24:82
 MfgRevision.....00:23:24:82
 Platform Name.....AOM-SXM5-IO

 Device ID(5)
```

```
Device Name.....SwitchPlx5
Chip Vendor.....Broadcom
Work Mode.....Synthetic Mode
Generation.....5
FW version.....04:11:00:00
SBR version.....00:23:24:82
MfgRevision.....00:23:24:82
Platform Name.....AOM-SXM5-IO
```

**The console output contains the following information** for the Broadcom chipset on the X13DEG-OA system.

```
Managed system.....localhost
PCIe Switch Device Vendor..... 172.31.33.118
 Device ID(0)
 Device Name.....SwitchBoard_1_PCIeSwitch_4
 FW Version.....04.12.00.00
```



#### Notes:

- This command is available on H12DGQ-NT6 with Broadcom PCIe Switch Gen4 Series chipsets, X13DEG-PVC with Broadcom PCIe Switch Gen5 Series chipsets and X12DSC-6 with Microchip PCIe Switch Gen4 Series chipsets platforms.
- On the H12DGQ-NT6 and X13DEG-PVC platforms with Broadcom PCIe Switch chipsets, find the readme.txt in the “SAA/driver/broadcom/PlxSdk” folder to load the device driver.
- On the X12DSC-6 platform with Microchip PCIe Switch Gen4 Series chipsets, download the SDK from [Microsemi](#) and follow the instructions on the website to load the device driver.
- Supported Operating System: Ubuntu 20.04 and later.
- The build device driver environment must have installed packages such as cmake and gcc.

### 5.10.2. Updating the PCIe Switch Firmware Image

Use the “UpdatePCleSwitch” command with the PCIe Switch firmware image to update the PCIe Switch firmware of a managed system.

**Single System**

OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdatePCleSwitch [--dev_id <index>] [--file <filename>]
In-Band	saa -c UpdatePCleSwitch [--dev_id <index>] [--file <filename>]

Example:

#### In-Band:

```
[SAA_HOME]# ./saa -c UpdatePCleSwitch --file fw_file.img --dev_id 0
```

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdatePCleSwitch --file fw_file.fw --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
```

**The console output contains the following information** for the Broadcom chipset with base mode on the X13DEG-PVC system.

```
Managed system.....localhost
 Device ID(0)
 Device Name.....SwitchPlx0
 Chip Vendor.....Broadcom
 Work Mode.....Base Mode
 Generation.....5
 Subsystem ID.....0072
 SBR version.....00161176

Local Firmware
File.....AOM_DP801_SW_bSW_SHP.sbr.FwTableTmp.hash.signed.bin
 Chip Vendor.....Broadcom
 Work Mode.....Base Mode
 Generation.....5
 SBR Version.....0016BAB0

Update firmware progress Started ...
Writing Firmware (100%)
Update firmware progress Finished.
Update firmware success.

Note: Please do power cycle to activate the updated image.
```

**The console output contains the following information** for the Broadcom chipset with synthetic mode on the X13DEG-PVC system.

```
Managed system.....localhost
 Device ID(3)
```



- The build device driver environment must have installed packages such as cmake and gcc.

## 5.11. Applications

### 5.11.1. Sending an IPMI/IPMB Raw Command

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

#### 5.11.1.1. IPMI Raw Command

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c RawCommand --raw <raw command>
In-Band	saa -c RawCommand --raw <raw command>
Multiple System	
OOB	saa -l <system list file> [-u <username> -p <password>] -c RawCommand --raw <raw command>

Example:

#### OOB:

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

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

#### In-Band:

```
[SAA_HOME]# ./saa -c RawCommand --raw '06 01'
```

```
[SAA_HOME]# ./saa -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
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c RawCommand --raw
'06 01'
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c RawCommand --raw
'0x06 0x01'
```

```
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.

### 5.11.1.2. IPMB Raw Command

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c RawCommand --ipmb <raw command>
In-Band	saa -c RawCommand --ipmb <raw command>
Multiple System	
OOB	saa -l <system list file> [-u <username> -p <password>] -c RawCommand --ipmb <raw command>

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c RawCommand --
ipmb '00 2C 2E D3 57 01 00 10'
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c RawCommand --
ipmb '0x00 0x2C 0x2E 0xD3 0x57 0x01 0x00 0x10'
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c RawCommand --ipmb '00 2C 2E D3 57 01 00 10'
```

```
[SAA_HOME]# ./saa -c RawCommand --ipmb '0x00 0x2C 0x2E 0xD3 0x57 0x01
0x00 0x10'
```

**The console output contains the following information.**

```
00
57 01 00 4C 00
```

#### **Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c RawCommand --ipmb
'00 2C 2E D3 57 01 00 10'
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c RawCommand --ipmb
'0x00 0x2C 0x2E 0xD3 0x57 0x01 0x00 0x10'
```

```
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.



**Note:** A raw command must be in quotation marks.

---

## **5.11.2. USB Port Accessibility Control**

---

In order to prevent security data from being leaked and unauthorized operations through USB ports, SAA has supported in-band USB port accessibility control for front and rear panels. Currently, SAA 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 contrast, 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 specification. 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 5.11.3 Getting USB Port Access Mode (Inband only)), or switched by running the command “SetUsbAccessMode” (see 5.11.4 Dynamic Control USB Port Access Mode (Inband only)). The mapping relationship 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

### 5.11.3. Acquiring USB Port Access Mode (Inband Only)

---

Use the in-band command “GetUsbAccessMode” command to get USB access mode in the running operating system. Currently, SAA 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 disabled 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.

Single System	
In-Band	saa -c GetUsbAccessMode

Example:

**In - Band :**

```
[SAA_HOME]# ./saa -c GetUsbAccessMode
```

**The console output contains the following information.**

```
[USB access mode]
REAR panel.....dynamic enabled
FRONT panel.....static disabled
```

#### 5.11.4. Dynamically Controlling 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.

Single System	
In-Band	saa -c SetUsbAccessMode --panel <front rear> {--disable   --enable}

---

Example:

**In-Band :**

```
[SAA_HOME]# ./saa -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, SAA 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.

---

### 5.11.5. 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. Users can save and configure the specific OEM functions for KMS features by using the [--file] option.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c KmsManage [--current_password <current password>   --cur_pw_file <current password filename>] [options...]
In-Band	saa -c KmsManage [--current_password <current password>   --cur_pw_file <current password filename>] [options...]
Multiple Systems	
OOB	saa -l <system list file> -u <username> -p <password> -c KmsManage [--current_password <current password>   --cur_pw_file <current password filename>] [options...]



Option	Augument	Desciption
--server_ip	<server IP address>	Enters a KMS server IP address.
--second_server_ip	<second server IP address>	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>	Enters client private key Password.
--file	<file name>	If 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. 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:

**00B:**

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

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

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

**In-Band:**

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -c KmsManage --action DeleteAll --reboot
```

```
[SAA_HOME]# ./saa -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 Certificate.....Uploaded
Client Private Key.....Uploaded
KMS Server Probe Status.....KMS function works normally
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c KmsManage --action
GetInfo
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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:

- 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.

---

### 5.11.6. SOL

Use the “SOL” command to activate SOL or setup the SOL configuration.

Action	Description
Activate	Activates SOL.
Deactivate	Stops SOL.
GetInfo	Gets SOL information.
Set	Sets SOL transmission bit rate, retry counts and retry interval.

With the “Activate” action, you can turn on SOL in the current text mode, and then press the <F12> key to exit. In order to display the remote text console, support for ANSI/VT100 terminal control escape sequences is required for the computer terminal or terminal emulator to run SAA. With the “Set” action and the following options, you can configure the SOL parameters.

Option	Description
--bitrate	Sets SOL transmission bit rate. Available SOL bit rates: [9.6 19.2 38.4 57.6 115.2] (kbps)
--retryCount	Sets SOL retry counts.
--retryInterval	The interval for BMC to retry sending SOL packets to the remote console. The retry interval is set in milliseconds, and the value should be ten or a multiple of ten.

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SOL --action &lt;action&gt; [--bitrate &lt;bitrate&gt;] [--retryCount &lt;retry count&gt;] [--retryInterval &lt;retryinterval&gt;]]</code>

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SOL --action <action> [--bitrate <bitrate>] [--retryCount <retry count>] [--retryInterval <retryinterval>]]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SOL --action
Activate
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SOL --action
Set --bitrate 115.2
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SOL --action Set -
-retryCount 3
```

```
SList.txt:
192.168.34.56
192.168.34.57
```



#### Notes:

- Command SOL does not support local in-band usage.
- Action activate does not support multiple system usage.

### 5.11.7. Invoking the Redfish API

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

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c RedfishApi --api <api path> [-v] [--request <http method>] [--file <file name> [--overwrite]] [--data <request body>] [--retry <number>]

In-Band	saa -l Redfish_HI -u <username> -p <password> -c RedfishApi --api <api path> [-v] [--request <http method>] [--file <file name> [--overwrite]] [--data <request body>] [--retry <number>]
<b>Multiple Systems</b>	
OOB	saa -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]

Option	Augument	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>	Outputs the response to file instead of printing on screen.
--overwrite	N/A	Overwrites the output file.
--data	<request body>	<p>The request body for the POST and PATCH methods.</p> <p>There are two usages:</p> <ul style="list-style-type: none"> <li>Supplies the body in string directly. Note that the special character should be escaped.</li> <li>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."</li> </ul>

Example:

**OOB:**

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

---

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

```
[SAA_HOME]# ./saa -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:**

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

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

```
[SAA_HOME]# ./saa -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
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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, SAA 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.

## **5.11.8. Remote Execution**

---

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

Single System	
Remote In-Band	saa -I Remote_INB --oi <OS IP or host name> --ou <OS username> --op <OS password> -c RemoteExec --remote_cmd <shell command> [-file <file name>]
Multiple Systems	
Remote In-Band	saa -I Remote_INB -l <system list file> -c RemoteExec --remote_cmd <shell command> [--file <file name>]

Example:

**Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c RemoteExec --remote_cmd "ls ~/supermicro/saa_remote_inband/ -l | grep test.sh" --file test.sh
```

**Multiple Systems Remote In-Band:**

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c RemoteExec --remote_cmd "ls ~/supermicro/saa_remote_inband/ -l | grep test.sh" --file test.sh
```

```
SList.txt:
192.168.34.56 root 111111
192.168.34.57 root 111111
```

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 stderr in the remote system will be redirected to stdout.
  - For use with tested third-party tools, please refer to Appendix K. Using SAA to Run 3rd -Party Tools.
-



---

### 5.11.9. Finding BMC Devices (Inband Only)

Use the “FindBmcDevices” command to find the available BMC devices within the given network segment or within the same network (255.255.255.0) of the network interface in the managed system. If the “--getMACs” option is used, the MAC addresses of the found devices would also being displayed and saved to file. **Syntax:**

Without --getMACs	
In-Band	saa -c FindBmcDevices [--start_ip <IP>]{--end_ip <IP>}{--netmask <netmask>}]
With --getMACs	
In-Band	saa -c FindBmcDevices --getMACs [--start_ip <IP>]{--end_ip <IP>}{--netmask <netmask>}{--file <filename>} [ {--find_user <username>}{--find_password <password>}]

Example:

**In - Band :**

```
[SAA_HOME]# ./saa -c FindBmcDevices --start_ip 192.168.34.0 --end_ip 192.168.34.255 --netmask 255.255.255.0
```

```
[SAA_HOME]# ./saa -c FindBmcDevices --start_ip 192.168.34.56 --end_ip 192.168.34.200 --netmask 255.255.255.0 --file 123.txt --getMACs
```

**The console output contains the following information.**

**[Without getMACs]**

```
Finding available BMC Devices
.....
.....
10.182.17.5 IPMI
10.182.17.6 X12 AST2600RoT
10.182.17.7 AST2500
...
10.182.17.8 X12 AST2600RoT
10.182.17.9 X12 AST2600RoT
37 BMC device(s) found.
```

## [With getMACs]

```
Finding available BMC Devices
.....
.....
.....
.....
3C:EC:EF:E2:57:E3 10.182.17.5 IPMI
3C:EC:EF:33:D4:D6 10.182.17.6 X12 AST2600RoT
AC:1F:6B:D5:8F:E2 10.182.17.7 AST2500
3C:EC:EF:E1:D6:16 10.182.17.8 X13 AST2600RoT
3C:EC:EF:D1:8A:44 10.182.17.9 X12 AST2500
3C:EC:EF:78:19:78 10.182.17.10 M12
3C:EC:EF:09:54:C1 10.182.17.11 X12 AST2600RoT
29 BMC device(s) found 123 was created.
10.184.17.12 cannot login by ADMIN/ADMIN
10.184.17.13 cannot login by ADMIN/ADMIN
```

### 5.11.10. Managing Found BMC Devices (Inband Only)

Use the “FoundBmcDevices” command to manage found BMC devices.

Action	Description
List	Lists all found BMC devices.
Clear	Clears all found BMC devices.
Copy	Copies the found devices to the default managed group.
CopyAll	Copies all found devices to the default managed group.
SaveAs	Saves the results of found BMC devices to a file.
Refresh	Refreshes the result of found BMC devices.

Single System	
In-Band	saa -c FoundBmcDevices --action { List   Clear   Copy --index <number seperated by space>   CopyAll   SaveAs --file <file name>   Refresh }

Example:

---

### In-Band :

```
[SAA_HOME]# ./saa -c FoundBmcDevices --action List
```

```
[SAA_HOME]# ./saa -c FoundBmcDevices --action Clear
```

The console output contains the following information.

#### [Action List]

```
Managed hosts loaded.Found hosts loaded.
```

```
Found IPMI Devices
```

```

```

Index	IP	Board	DC Room	Row Rack	Num Type	BMC
1	169.254.3.254					
2	10.184.3.166					
3	10.184.3.170					
4	10.184.3.185					

```
4 IPMI device(s) found.
```

#### [Action Clear]

```
Managed hosts loaded.Found hosts loaded.Done
```

### 5.11.11. Shell Mode

Use the “Shell” command to enter Shell Mode. In this mode, you can run multiple commands on a managed server without exiting the SAA tool. The related information in the prompt is provided for your reference.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c Shell

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c Shell
```

The console output contains the following information.

```
Press Ctrl+D or "exit" to exit
Press "?" or "help" for help
Press UP and DOWN key for command history
ADMIN@192.168.34.56 X13SEI-TF/-F (S0/G0 Working, 83w, 01.01.05) 15:44
X13_RoT2.0_ATEN_AST2600_1_1>
```

In Shell Mode, you can execute multiple commands on the managed server as follows:

```
Press Ctrl+D or "exit" to exit
Press "?" or "help" for help
Press UP and DOWN key for command history
ADMIN@192.168.34.56 X13SEI-TF/-F (S0/G0 Working, 92w, 01.01.05) 16:39
X13_RoT2.0_ATEN_AST2600_1_1> GetBmcInfo

Managed system.....192.168.34.56
 BMC UFFN.....BMC_X13AST2600-ROT-C301MS_20231004_01.01.05_STDsp.bin
 BMC type.....X13_RoT2.0_ATEN_AST2600_1_1
 BMC version.....01.01.05
 BMC ext. version....01 00 00 (P)
 BMC build date.....2023/10/04
ADMIN@192.168.34.56 X13SEI-TF/-F (S0/G0 Working, 117w, 01.01.05) 16:39
X13_RoT2.0_ATEN_AST2600_1_1> GetBiosInfo

Managed system.....192.168.34.56
 Board ID.....1C56
 BIOS build date.....2023/09/18
 BIOS version.....1.5
ADMIN@192.168.34.56 X13SEI-TF/-F (S0/G0 Working, 83w, 01.01.05) 16:39
X13_RoT2.0_ATEN_AST2600_1_1> exit
Bye~
```

### 5.11.12. Prompt

Use the "Prompt" command to configure the current status of the managed system in the prompt. The configuration will be stored in the "saa\_prompt.properties" file, which is located at SAA\_HOME directory, and recalled at the next startup.

Single System	
In-Band	saa -c Prompt --action <action> --item <prompt item> [--enable   --disable]

---

Example:

**In-Band :**

```
[SAA_HOME]# ./saa -c Prompt --action Get --item all
```

**The console output contains the following information.**

```
prompt_time: on
prompt_fwVer: on
prompt_username: on
prompt_ip: on
prompt_mb_name: on
prompt_powerW: on
prompt_acpi: on
```

```
[SAA_HOME]# ./saa -c Prompt --action Set --item time --disable
```

**The console output contains the following information.**

```
Prompt status for time is set for saa_prompt.properties.
```

```
[SAA_HOME]# ./saa -c Prompt --action Get --item time
```

**The console output contains the following information.**

```
prompt_time: off
```

When you enter the Shell Mode after this, you will see the default prompt listings as follows:

```
ADMIN@192.168.34.56 X13SEI-TF/-F (S0/G0 Working,83w,01.01.05) 15:44
X13_RoT2.0_ATEN_AST2600_1_1>
(A) (B) (C) (D) (E) (F) (G)
(H)
(A) Username
(B) IP address
(C) Motherboard
(D) ACPI status
(E) Power consumption
```

---

```
(F) IPMI firmware version
(G) Current time
(H) IPMI firmware type
```

If the information is not displayed even when the item is set to "on," it means that SAA cannot retrieve the correct data.

### 5.11.13. Launching Remote Console

Use the "RemoteConsole" command to launch the remote managed system.

Single System	
OoB	saa -i <IP or host name> -u <username> -p <password> -c RemoteConsole

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c RemoteConsole
```

### 5.11.14. Getting USB Host Controller Information

Use the "GetUSBHostControllerInfo" command to get and read the USB Host Controller information of the managed system, and parse USB Host Controller information from the firmware and configuration files.

Single System	
In-Band	saa -c GetUSBHostControllerInfo [--file <filename> --cfg_file <cfgfilename> [--file_only]]

Example:

**In - Band :**

```
[SAA_HOME]# ./saa -c GetUSBHostControllerInfo
```

---

```
[SAA_HOME]# ./saa -c GetUSBHostControllerInfo --file fw_file.mem --
file_only
```

```
[SAA_HOME]# ./saa -c GetUSBHostControllerInfo --cfg_file cfg_file.ini --
file_only
```

**The console output contains the following information** for the Renesas  $\mu$ PD720201 chipset on the X14SBT-G system.

```
Managed system.....localhost
 Device ID(0)
 Address(Bus-Dev-Func).....15-00-00
 FW Version.....2.0.2.6
 Revision.....3
 PCI Subsystem ID.....FFFF
 PCI Subsystem Vendor ID.....FFFF

 Device ID(1)
 Address(Bus-Dev-Func).....18-00-00
 FW Version.....2.0.2.6
 Revision.....3
 PCI Subsystem ID.....FFFF
 PCI Subsystem Vendor ID.....FFFF

 Firmware File.....K2024090.mem
 FW Version.....2.0.2.4

 Config File.....cfg201v3.ini
 SubSystem Vendor ID.....FFFF
 SubSystem ID.....FFFF
```



**Notes:**

- This command is available on the X14SBT-G platform with the Renesas  $\mu$ PD720201 USB Host Controller chipset.
  - On the X14SBT-G platform with Renesas USB Host Controller  $\mu$ PD720201 chipset, execute the "make -f Makefile.drv" command in the "SAA/driver/renesas/USB" folder to build the device driver.
  - Supported operating systems include Ubuntu 20.04 and later, Red Hat 9.0 and later.
  - The device driver build environment must have packages such as cmake and gcc installed.
-

---

### 5.11.15. Updating the USB Host Controller Firmware Image

Use the “UpdateUSBHostController” command with the USB Host Controller firmware image to update the USB Host Controller firmware of a managed system.

Single System	
In-Band	saa -c UpdateUSBHostController [--dev_id <index>] [--file <filename.mem>] [--cfg_file <filename.ini>] [--reboot]

Example:

**In-Band :**

```
[SAA_HOME]# ./saa -c UpdateUSBHostController --file fw_file.mem --
cfg_file cfg_file.ini --dev_id 0
```

**The console output contains the following information** for the Renesas  $\mu$ PD720201 chipset on the X14SBT-G system.

```
Managed system.....localhost
 Device ID(0)
 Address(Bus-Dev-Func).....15-00-00
 FW Version.....2.0.2.6
 Revision.....3
 PCI Subsystem ID.....FFFF
 PCI Subsystem Vendor ID.....FFFF

 Firmware File.....K2024090.mem
 FW Version.....2.0.2.4

 Config File.....cfg201v3.ini
 SubSystem Vendor ID.....FFFF
 SubSystem ID.....FFFF

Start to update firmware.
Erase Serial ROM completed.
Write Serial ROM completed.
Verify Serial ROM completed.
Update firmware succeeded.

Note: Please do power cycle to activate the updated image.
```



**Notes:**

- This command is available on X14SBT-G with Renesas USB Host Controller  $\mu$ PD720201 chipset platform.
- On the X14SBT-G platform with Renesas USB Host Controller  $\mu$ PD720201 chipset, execute command "make -f Makefile.drv" in the "SAA/driver/renesas/USB" folder to build the device driver.
- Supported Operating System: Ubuntu 20.04 and later , Redhat 9.0 and later.
- The build device driver environment must have installed packages such as cmake and gcc.

### 5.11.16. Remote Screenshot

Use the "RemoteScreenshot" command to get a screenshot of the remote managed system and save it as a PNG file.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c RemoteScreenshot --file <filename.png>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
RemoteScreenshot --file remotefile.png
```

**Notes:**

- The RemoteScreenshot command can only be executed on Windows and Linux systems.
- For Windows systems in standby mode, execute the RemoteScreenshot command twice.

### 5.11.17. Remote Keyboard Operation

Use the “RemoteKeyboard” command to send keyboard operations to the remote managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c RemoteKeyboard [--file <keyboard.txt>] [--showall]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c RemoteKeyboard
--file keyboard.txt
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c RemoteKeyboard
--showall
```

#### In-Band:

```
[SAA_HOME]# ./saa -c RemoteKeyboard --showall
```

**The console output contains the following information for the supported keys of Remote Keyboard.**

```
=====
| Remote Keyboard |
|=====|
Remote Keyboard Parameters List

Alphanumeric Keys : A-Z, a-z, 0-9, Symbols Keys (example: ,./!#%& ... etc)
Modifier Keys : [Shift], [Ctrl], [Alt], [Win]
Navigation Keys : [Up], [Down], [Left], [Right], [PageUp], [PageDown],
 [Home], [End]
Editing Keys : [Enter], [Backspace], [Insert], [Delete], [Tab], [Space]
Miscellaneous Keys: [PrtSc], [Pause], [Esc], [F1]-[F12]
Macro Key example : [Ctrl+Alt+Delete], [Alt+F4], [Ctrl+v] ... etc
Delay Parameter : [Delay=?h?m?s], [Delay=?m?s], [Delay=?s]

Remote Keyboard File Sample

[Ctrl+Alt+Delete][Delay=5s]
password[Enter][Delay=10s]
```

```
cmd[Enter][Delay=1s]
ipconfig[Enter]
```

**Note:**

The RemoteKeyboard command only can be executed on Windows and Linux operating systems.

## 5.12. GPU Management

### 5.12.1. Getting GPU Information

Use the “GetGpuInfo” command to get the current GPU information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetGpuInfo [--show_all] [--showoam <oam id>] [--file <filename>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetGpuInfo [--show_all] [--showoam <oam id>] for Intel Gaudi2/3: saa -c GetGpuInfo [--show_all] [--file <filename>] [--showoam <oam id>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetGpuInfo [--show_all] [--showoam <oam id>] [--file <filename>] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c GetGpuInfo [--showoam <oam id>] [--file <filename>]
Remote In-Band	saa -I Redfish_HI -I <system list file> -c GetGpuInfo [--show_all] [--showoam <oam id>] [--file <filename>] [--remote_saa <remote SAA path>]

Example:

---

**00B:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetGpuInfo
```

**In-Band:**

```
[SAA_HOME]# ./saa -c GetGpuInfo
```

**In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetGpuInfo
```

**The console output contains the following information** of the managed system with add-on GPU cards installed.

```
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 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
```

**The console output contains the following information** for HGX H100 system on X13/H13 systems.

```
Managed system.....192.168.34.56
 HGX Model.....HGX H100 8-GPU
 HMC
 version.....HGX-22.10-1-rc31
 ERoT version.....00.02.0120.0000_n00
 FPGA
 version.....2.0E
 ERoT version.....00.02.0120.0000_n00
 PCIe Switch
 version.....1.7.5F
 ERoT version.....00.02.0120.0000_n00
 GPU SXM [1]
 version.....96.00.61.00.01
 ERoT version.....00.02.0120.0000_n00
 GPU SXM [2]
 version.....96.00.61.00.01
 ERoT version.....00.02.0120.0000_n00
 GPU SXM [3]
 version.....96.00.61.00.01
 ERoT version.....00.02.0120.0000_n00
 GPU SXM [4]
 version.....96.00.61.00.01
 ERoT version.....00.02.0120.0000_n00
 GPU SXM [5]
 version.....96.00.61.00.01
 ERoT version.....00.02.0120.0000_n00
 GPU SXM [6]
 version.....96.00.61.00.01
 ERoT version.....00.02.0120.0000_n00
 GPU SXM [7]
 version.....96.00.61.00.01
 ERoT version.....00.02.0120.0000_n00
 GPU SXM [8]
 version.....96.00.61.00.01
 ERoT version.....00.02.0120.0000_n00
 NVSwitch [0]
 version.....96.10.35.00.01
 ERoT version.....00.02.0120.0000_n00
 NVSwitch [1]
 version.....96.10.35.00.01
 ERoT version.....00.02.0120.0000_n00
 NVSwitch [2]
```

```

version.....96.10.35.00.01
ERoT version.....00.02.0120.0000_n00
NVSwitch [3]
version.....96.10.35.00.01
ERoT version.....00.02.0120.0000_n00
PCiE Retimer [0]
version.....1.31.X
PCiE Retimer [1]
version.....1.31.X
PCiE Retimer [2]
version.....1.31.X
PCiE Retimer [3]
version.....1.31.X
PCiE Retimer [4]
version.....1.31.X
PCiE Retimer [5]
version.....1.31.X
PCiE Retimer [6]
version.....1.31.X
PCiE Retimer [7]
version.....1.31.X
HGX information
=====
[UBB (1)]
Name : GPU Baseboard
Model : HGX_H100
Manufacturer : NVIDIA
Serial Number : 1664922651034
Part Number : 935-24287-0000-000
Chassis Type : Zone

[GPU(1)]
Location : 1
Model : H100 80GB HBM3
Serial Number : 1655022001438
Part Number : 2330-885-A1
Firmware Version : 96.00.46.00.0E
Temperature(C) : 43 degreeC
/** Please refer to Note 2 **/
[HGX Delta System Temperature]
[HBM]
Reading Temperature : 34 degreeC
HBM 1 Temperature : 34 degreeC
HBM 2 Temperature : 30 degreeC
HBM 3 Temperature : 32 degreeC
HBM 4 Temperature : 34 degreeC
HBM 5 Temperature : 34 degreeC
HBM 6 Temperature : 31 degreeC
HBM 7 Temperature : 31 degreeC
HBM 8 Temperature : 34 degreeC
/** Please refer to Note 3 **/

```



---

**The console output contains the following information** of the managed system with Intel Gaudi2 GPU cards installed.

```
Managed system.....localhost
 Habana UBB CPLD version.....000A0A02
 Habana OAM CPLD version
 Device Id(0)
 Version.....0F
 Configuration ID.....01

 Device Id(1)
 Version.....0F
 Configuration ID.....01

 Device Id(2)
 Version.....0F
 Configuration ID.....01

 Device Id(3)
 Version.....0F
 Configuration ID.....01

 Device Id(4)
 Version.....0F
 Configuration ID.....01

 Device Id(5)
 Version.....0F
 Configuration ID.....01

 Device Id(6)
 Version.....0F
 Configuration ID.....01

 Device Id(7)
 Version.....0F
 Configuration ID.....01
 SPI Firmware Version:
 Device ID.....b3:00.0
 OAM ID.....0
 Serial Number.....AM27043716
 Module ID.....6
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

 Device ID.....cc:00.0
 OAM ID.....1
 Serial Number.....AM30032490
 Module ID.....4
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```

Device ID.....b4:00.0
 OAM ID.....2
 Serial Number.....AM27043737
 Module ID.....7
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

Device ID.....cd:00.0
 OAM ID.....3
 Serial Number.....N/A
 Module ID.....N/A
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.9.0-fw-
42.0.1-sec-3 (Mar 06 2023 - 23:23:58)

Device ID.....1a:00.0
 OAM ID.....4
 Serial Number.....N/A
 Module ID.....N/A
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.9.0-fw-
42.0.1-sec-3 (Mar 06 2023 - 23:23:58)

Device ID.....19:00.0
 OAM ID.....5
 Serial Number.....AM30032493
 Module ID.....2
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

Device ID.....43:00.0
 OAM ID.....6
 Serial Number.....AM30032518
 Module ID.....0
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

Device ID.....44:00.0
 OAM ID.....7
 Serial Number.....AM27043781
 Module ID.....1
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

```

**The console output contains the following information** of the managed system with Intel Gaudi3 GPU cards installed.

```

Managed system.....localhost
 Device.....0000:17:00.0
 Product Name.....HL-325
 Model Number.....F08GL0DIG013A

```

```

Serial Number.....A015019764
Module ID.....0
Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)
Firmware [OS] Version.....Zephyr 2.7.2-hl-gaudi3-1.17.0-fw-51.0.1-
sec-0 (Jun 30 2024 - 00:35:07)
OAM CPLD Version.....0x65f08d7c00000003
PCB Assembly Version.....V3A
PCB Version.....R0B
HL Revision.....0
AIP UUID.....01P4-0A0903LH-18-U2W757-22-09-05

Device.....0000:97:00.0
Product Name.....HL-325
Model Number.....F08GL0DIG013A
Serial Number.....A015019708
Module ID.....4
Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)
Firmware [OS] Version.....Zephyr 2.7.2-hl-gaudi3-1.17.0-fw-51.0.1-
sec-0 (Jun 30 2024 - 00:35:07)
OAM CPLD Version.....0x65f08d7c00000003
PCB Assembly Version.....V3A
PCB Version.....R0B
HL Revision.....0
AIP UUID.....01P4-0A0903LH-18-U2W757-03-12-04

Device.....0000:2c:00.0
Product Name.....HL-325
Model Number.....F08GL0DIG013A
Serial Number.....A015019836
Module ID.....1
Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)
Firmware [OS] Version.....Zephyr 2.7.2-hl-gaudi3-1.17.0-fw-51.0.1-
sec-0 (Jun 30 2024 - 00:35:07)
OAM CPLD Version.....0x65f08d7c00000003
PCB Assembly Version.....V3A
PCB Version.....R0B
HL Revision.....0
AIP UUID.....01P4-0A0903LH-18-U2W736-08-00-04

Device.....0000:3d:00.0
Product Name.....HL-325
Model Number.....F08GL0DIG013A
Serial Number.....A015019768
Module ID.....2
Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)
Firmware [OS] Version.....Zephyr 2.7.2-hl-gaudi3-1.17.0-fw-51.0.1-
sec-0 (Jun 30 2024 - 00:35:07)
OAM CPLD Version.....0x65f08d7c00000003
PCB Assembly Version.....V3A

```

```

 PCB Version.....R0B
 HL Revision.....0
 AIP UUID.....01P4-0A0903LH-18-U2Y666-01-04-06

Device.....0000:a9:00.0
 Product Name.....HL-325
 Model Number.....F08GL0DIG013A
 Serial Number.....A015019755
 Module ID.....5
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)
 Firmware [OS] Version.....Zephyr 2.7.2-hl-gaudi3-1.17.0-fw-51.0.1-
sec-0 (Jun 30 2024 - 00:35:07)
 OAM CPLD Version.....0x65f08d7c00000003
 PCB Assembly Version.....V3A
 PCB Version.....R0B
 HL Revision.....0
 AIP UUID.....01P4-0A0903LH-18-U2Y666-01-05-00

Device.....0000:ba:00.0
 Product Name.....HL-325
 Model Number.....F08GL0DIG013A
 Serial Number.....A015019860
 Module ID.....6
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)
 Firmware [OS] Version.....Zephyr 2.7.2-hl-gaudi3-1.17.0-fw-51.0.1-
sec-0 (Jun 30 2024 - 00:35:07)
 OAM CPLD Version.....0x65f08d7c00000003
 PCB Assembly Version.....V3A
 PCB Version.....R0B
 HL Revision.....0
 AIP UUID.....01P4-0A0903LH-18-U2W736-13-05-04

Device.....0000:cb:00.0
 Product Name.....HL-325
 Model Number.....F08GL0DIG013A
 Serial Number.....A015019865
 Module ID.....7
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)
 Firmware [OS] Version.....Zephyr 2.7.2-hl-gaudi3-1.17.0-fw-51.0.1-
sec-0 (Jun 30 2024 - 00:35:07)
 OAM CPLD Version.....0x65f08d7c00000003
 PCB Assembly Version.....V3A
 PCB Version.....R0B
 HL Revision.....0
 AIP UUID.....01P4-0A0903LH-18-U2W736-08-00-05

Device.....0000:4e:00.0
 Product Name.....HL-325
 Model Number.....F08GL0DIG013A
 Serial Number.....A015019869

```

```
Module ID.....3
Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)
Firmware [OS] Version.....Zephyr 2.7.2-hl-gaudi3-1.17.0-fw-51.0.1-
sec-0 (Jun 30 2024 - 00:35:07)
OAM CPLD Version.....0x65f08d7c00000003
PCB Assembly Version.....V3A
PCB Version.....R0B
HL Revision.....0
AIP UUID.....01P4-0A0903LH-18-U2W736-05-09-01
```

**The console output contains the following information** of the managed system with NVIDIA GH200 GPU cards installed.

```
Managed system.....192.168.34.56
GPU information
=====
[GPU(0)]
 Location : 0
 GPU Vendor : NVIDIA
 Model : GH200 480GB
 Serial Number : 1642723000173
 Part Number : 2342-888-A1
 Firmware Version : 96.00.84.00.02
 PCIe Type : Gen4
 Max PCIe Type : Gen5
 Lanes In Use : 1
 Max Lanes : 1
 UUID : 3949b757-be6b-568c-88f4-5a833404cb8c
 Max Speed : 1980 MHz
 Min Speed : 345 MHz
 Operating Speed : 690 MHz
```

**The console output contains the following information** of the managed system with AMD MI300X GPU cards installed.

```
Managed system.....196.168.34.56
Model.....AMD Instinct MI300X UBB
 SMC
 version.....t28_v2.11.0.32
 SMC FPGA
 version.....T28_S_v0.0C.0.73803c2d
 UBB Bundle
 version.....BKC_X23.44.09.76
 GPU IFWI
 version.....vBRP018G_85284
 Retimers
```

```
version.....v2_8_76
OAM RM
version.....v4_0_9
ROT
version.....aa04
UBB FPGA
version.....v0.21.2.a657321d
```

**The console output contains the following information** for Redstone-Next Sytem.

```
Managed system.....196.168.34.56
HGX information
=====
[GPU (1)]
Location : 1
PCIe Type : Gen-1
Lanes In Use : -1
Max Lanes : -1
Temperature(C) : 0 degreeC

[GPU (2)]
Location : 2
PCIe Type : Gen-1
Lanes In Use : -1
Max Lanes : -1
Temperature(C) : 0 degreeC

[GPU (3)]
Location : 3
PCIe Type : Gen-1
Lanes In Use : -1
Max Lanes : -1
Temperature(C) : 0 degreeC

[GPU (4)]
Location : 4
PCIe Type : Gen-1
Lanes In Use : -1
Max Lanes : -1
Temperature(C) : 0 degreeC

[HGX Redstone System Temperature]
[HBM]
Reading Temperature : 0 degreeC
HBM 1 Temperature : 0 degreeC
HBM 2 Temperature : 0 degreeC
HBM 3 Temperature : 0 degreeC
HBM 4 Temperature : 0 degreeC
[FPGA]
Reading Temperature : 0 degreeC
```

```
[GPU Board]
 Reading Temperature : 0 degreeC
[ReTimer]
 Reading Temperature : 38 degreeC

[OnBoard_Retimer_1]
 Dev_ID : 1
 Version : 2.3.0
[OnBoard_Retimer_2]
 Dev_ID : 2
 Version : 2.3.0
[OnBoard_Retimer_3]
 Dev_ID : 3
 Version : 2.3.0
[OnBoard_Retimer_4]
 Dev_ID : 4
 Version : 2.3.0
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetGpuInfo
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

**The console output contains the following information** of the managed system with Intel Gaudi3 GPU cards installed.

```
Managed system.....10.141.176.170
OAM 1:
 UBB_1_Retimer_1 version.....2.8.45
OAM 2:
 UBB_1_Retimer_2 version.....2.8.45
OAM 3:
 UBB_1_Retimer_3 version.....2.8.45
OAM 4:
 UBB_1_Retimer_4 version.....2.8.45
OAM 5:
 UBB_1_Retimer_5 version.....2.8.45
OAM 6:
 UBB_1_Retimer_6 version.....2.8.45
OAM 7:
 UBB_1_Retimer_7 version.....2.8.45
OAM 8:
```

```
UBB_1_Retimer_8 version.....2.8.45
UBB CPLD Version.....00.0C
```

## Remote In-Band:

**The console output contains the following information** of the managed system with Intel Gaudi2 GPU cards installed.

```
Managed system.....localhost
Habana UBB CPLD version.....000A0A02
Habana OAM CPLD version
 Device Id(0)
 Version.....0F
 Configuration ID.....01

 Device Id(1)
 Version.....0F
 Configuration ID.....01

 Device Id(2)
 Version.....0F
 Configuration ID.....01

 Device Id(3)
 Version.....0F
 Configuration ID.....01

 Device Id(4)
 Version.....0F
 Configuration ID.....01

 Device Id(5)
 Version.....0F
 Configuration ID.....01

 Device Id(6)
 Version.....0F
 Configuration ID.....01

 Device Id(7)
 Version.....0F
 Configuration ID.....01
SPI Firmware Version:
 Device ID.....b3:00.0
 OAM ID.....0
 Serial Number.....AM27043716
 Module ID.....6
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```



```

Device ID.....cc:00.0
 OAM ID.....1
 Serial Number.....AM30032490
 Module ID.....4
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

Device ID.....b4:00.0
 OAM ID.....2
 Serial Number.....AM27043737
 Module ID.....7
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

Device ID.....cd:00.0
 OAM ID.....3
 Serial Number.....N/A
 Module ID.....N/A
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.9.0-fw-
42.0.1-sec-3 (Mar 06 2023 - 23:23:58)

Device ID.....1a:00.0
 OAM ID.....4
 Serial Number.....N/A
 Module ID.....N/A
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.9.0-fw-
42.0.1-sec-3 (Mar 06 2023 - 23:23:58)

Device ID.....19:00.0
 OAM ID.....5
 Serial Number.....AM30032493
 Module ID.....2
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

Device ID.....43:00.0
 OAM ID.....6
 Serial Number.....AM30032518
 Module ID.....0
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

Device ID.....44:00.0
 OAM ID.....7
 Serial Number.....AM27043781
 Module ID.....1
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

```

---

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.

---



**Notes:**

- For more details on support, please refer to the following links.
    1. [Supernova - Qualified Platform List for NVIDIA vGPU](#)
    2. [Supported GPU System Model](#)
    3. Appendix N. GetGpuInfo/UpdateGpu supported platform matrix
  - This part has omitted the same GPU information with different index.
  - This part has omitted the temperature information of FPGA, PCI Switch, PLX, ReTimer and NVSwitch.
  - On Intel PVC system, igsc must be installed to communicate with PVC\_IFWI and PVC\_PSCBIN devices.
  - On Intel Gaudi2/3 system, Habana libraries (hl-fw-loader and hl-smi) with ubuntu version 20.04 are required.
- 

### 5.12.2. Updating the GPU Firmware Image

Use the "UpdateGpu" command with the GPU firmware image (CEC/FPGA/HGX\_H100/H100\_FPGA/H100\_FPGA\_EROT/H100\_HMC/H100\_HMC\_EROT/H100\_PCIESWITCH/H100\_PCIESWITCH\_EROT/H100\_GPU/H100\_GPU\_EROT/H100\_NVSWITCH/H100\_NVSWITCH\_EROT/H100\_RETIMER/Intel\_Gaudi2/Intel\_Gaudi3/IntelPVC/MGX\_GPU/MI300X/ONBOARD\_RETIMER) to update the GPU firmware of a managed system by SAA.

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c UpdateGpu --item &lt;CEC FPGA HGX_H100 H100_FPGA H100_FPGA_EROT H100_HM C H100_HMC_EROT H100_PCIESWITCH H100_PCIESWITCH_ERO T H100_GPU H100_GPU_EROT H100_NVSWITCH H100_NVSWITC H_EROT H100_RETIMER PVC_RETIMER GAUDI_RETIMER PVC_A MC PVC_UBB_CPLD MGX_GPU MI300X ONBOARD_RETIMER &gt; -- file &lt;filename&gt; [--reboot] [--post_complete] [--dev_id &lt;device ID&gt;]  for Intel gaudi 3</pre>

	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c UpdateGpu --item &lt;GAUDI_UBB_CPLD GAUDI_RETIMER&gt; --file &lt;filename&gt; [--reboot]</pre>
In-Band	<pre>saa -l Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c UpdateGpu --item &lt;CEC FPGA HGX_H100 H100_FPGA H100_FPGA_EROT H100_HM C H100_HMC_EROT H100_PCIESWITCH H100_PCIESWITCH_ERO T H100_GPU H100_GPU_EROT H100_NVSWITCH H100_NVSWITC H_EROT H100_RETIMER PVC_RETIMER GAUDI_RETIMER PVC_A MC GAUDI_UBB_CPLD MI300X ONBOARD_RETIMER&gt; --file &lt;filename&gt; [--reboot] [--dev_id &lt;device ID&gt;]</pre> <p>for Intel gaudi 2</p> <pre>saa -c UpdateGpu --dev_id &lt;device_id&gt; --item &lt; GAUDI_OAM_CPLD  GAUDI_SPI PVC_IFWI PVC_PSCBIN &gt; --file &lt;filename&gt; [--reboot] [-- dev_id &lt;device ID&gt;]</pre> <p>for Intel gaudi 3</p> <pre>saa -c UpdateGpu --item &lt; GAUDI_OAM_CPLD  GAUDI_SPI &gt; --file &lt;filename&gt; [--reboot]</pre>
Remote In-Band	<pre>saa -l Remote_INB --oi &lt;IP address&gt; --ou &lt;username&gt; --op &lt;password&gt; -c UpdateGpu {--item &lt;GAUDI_OAM_CPLD GAUDI_UBB_CPLD GAUDI_SPI PVC_IFWI PV C_PSCBIN &gt; --file &lt;filename&gt;} [--reboot] [--remote_saa &lt;remote saa_location&gt;] [--dev_id &lt;device ID&gt;]</pre>
<b>Multiple Systems</b>	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c UpdateGpu {--item &lt;CEC FPGA HGX_H100 H100_FPGA PVC_RETIMER GAUDI_RETI MER PVC_AMC PVC_UBB_CPLD MGX_GPU MI300X H100_RETIM ER ONBOARD_RETIMER&gt; --file &lt;filename&gt;} [--reboot] [-- post_complete]] [--dev_id &lt;device ID&gt;]</pre> <p>for Intel gaudi 3</p> <pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c UpdateGpu --item &lt;GAUDI_UBB_CPLD GAUDI_RETIMER&gt; --file &lt;filename&gt; [--reboot]</pre>
Remote In-Band	<pre>saa -l Redish_HI -l &lt;system list file&gt; -c UpdateGpu {--item &lt;GAUDI_OAM_CPLD GAUDI_UBB_CPLD PVC_IFWI PVC_PSCBIN  GAUDI_SPI&gt; --file &lt;filename&gt;} [--reboot] [--remote_saa &lt;remote saa_location&gt;] [--dev_id &lt;device ID&gt;]</pre>

**00B:**

**The console output contains the following information.**

**OOB:**

SuperServer Automation Assistant User's Guide Page 560

```
.....Done

Updating HGX H100 FW...>>Done
.....
Status: HGX H100 is updated for 192.168.34.56

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: MemoryInitializationStarted

.....
.....
Status: PCIResourceConfigStarted

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

**00B:**

```
[SAA_HOME] ./saa -c updategpu -i 192.168.34.56 -u ADMIN -p QHKPSPALGW --item
PVC_Retimer --dev_id 3 --file pt516_x16_reversed_v2_7_0.bin
SuperServer Automation Assistant 1.0.0 (2023/11/07) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
.

Managed system.....192.168.34.56
PVC Retimer Version.....2.7.0
PVC Retimer image file..... /UBB_FW/Retimer/pt516_x16_reversed_v2_7_0.bin

Status: Start updating PVC Retimer for 192.168.34.56

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

Uploading PVC Retimer FW...Done

Updating PVC Retimer FW..>>>Done

Status: PVC Retimer is updated for 192.168.34.56
```

---

[illegible]



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

```

[illegible]

**OOB:**

```
Managed system.....10.141.176.170
Gaudi UBB CPLD Version.....00.0C
Gaudi UBB CPLD image file.....HLB-325_Primary_R0A_20240611a_FPGA_00_0c_RevD.svf
```

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

```

[illegible][illegible]

---

SuperServer Automation Assistant User's Guide Page 564



---

## In-Band :

```
[SAA_HOME]# ./saa -l Redfish_HI -u ADMIN -p PASSWORD -c UpdateGpu --file GPU_FPGA.bin --item FPGA
```

```
[SAA_HOME]# ./saa -l Redfish_HI -u ADMIN -p PASSWORD -c UpdateGpu --file NVIDIA_HGX_H100.pkg --item HGX_H100 --reboot
```

```
[SAA_HOME]# ./saa -c updategpu --dev_id 1 --file HL225_PFR_20230427_0F_644A7EDA_production.signed_cfg0.svf --item GAUDI_OAM_CPLD
```

```
SuperServer Automation Assistant 1.0.0 (2023/11/07) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
Start to Update firmware of the Habana OAM CPLD
.....
.....
.....
Done.
```

```
[SAA_HOME]# ./saa -c updategpu --item GAUDI_OAM_CPLD --file gaudi3-cpld-LFMX05-15D-03-TS66530567.itb
```

```
SuperServer Automation Assistant 1.1.0 (2024/07/17) (x86_64)
Copyright(C) 2024 Super Micro Computer, Inc. All rights reserved.
Start to Update firmware of the Gaudi 3

Unload Habana Driver.....

PLEASE DO NOT POWER OFF THE SYSTEM!!!
Updating gaudi3-cpld-LFMX05-15D-03-TS66530567.itb.....
.....
.....
.....
.....
[0000:17:00.0]:Ok (1012.400125 seconds)
[0000:97:00.0]:Ok (1012.400125 seconds)
[0000:2c:00.0]:Ok (1012.400125 seconds)
[0000:3d:00.0]:Ok (1012.400125 seconds)
[0000:a9:00.0]:Ok (1012.400125 seconds)
[0000:ba:00.0]:Ok (1012.400125 seconds)
[0000:cb:00.0]:Ok (1012.400125 seconds)
[0000:4e:00.0]:Ok (1012.400125 seconds)
```

---

```
Load Habana Driver.....
```

```
Done
```

```
[SAA_HOME]# ./saa -c updategpu --item PVC_UBB_CPLD --file Etron_UBB-
SA_CPLD1_A02.jed --dev_id 0
```

```
SuperServer Automation Assistant 1.0.0 (2023/11/07) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
```

```
Start to Update firmware of the Habana UBB CPLD
```

```
.....
```

```
..
```

```
Done.
```

```
[SAA HOME] ./saa -c updategpu --item gaudi_spi --file habanalabs-firmware-
odm-1.10.0-494.amd64.deb --dev_id cc:00.0
```

```
SuperServer Automation Assistant 1.0.0 (2023/11/07) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
```

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

```
Unload Habana Driver
```

```
.....
```

```
.....
```

```
Gaudi Write Disable Protection Enable
```

```
PLEASE DO NOT POWER OFF THE SYSTEM!!!
```

```
Gaudi Write Recovery Protection
```

```
Show SPI Firmware
```

```
.....
```

```
.. Device ID.....19:00.0
```

```
 OAM ID.....0
```

```
 Serial Number.....AM30032493
```

```
 Module ID.....2
```

```
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```
 Device ID.....b3:00.0
```

```
 OAM ID.....1
```

```
 Serial Number.....AM27043716
```

```
 Module ID.....6
```

```
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```
Device ID.....cc:00.0
 OAM ID.....3
 Serial Number.....AM30032490
 Module ID.....4
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```
Device ID.....43:00.0
 OAM ID.....4
 Serial Number.....AM30032518
 Module ID.....0
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```
Device ID.....44:00.0
 OAM ID.....5
 Serial Number.....AM27043781
 Module ID.....1
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```
Device ID.....b4:00.0
 OAM ID.....7
 Serial Number.....AM27043737
 Module ID.....7
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```
[SAA HOME] ./saa -c updategpu --item gaudi_spi --file habanalabs-firmware-
odm-1.17.0-343.amd64.deb
```

```
Managed system.....localhost
Start to Update SPI firmware of the Gaudi 3

Firmware Loading
Firmware Loaded: habanalabs-firmware-odm-1.17.0-343.amd64.deb
UnloadDriver
.....
Firmware Updating

PLEASE DO NOT POWER OFF THE SYSTEM!!!
.....
.....
.....
.....
.....
Firmware Updated:habanalabs-firmware-odm-1.17.0-343.amd64.deb

LoadDriver
....
```

```
.....
SPI-FW has been Updated.
 Device ID.....17:00.0
 OAM ID.....0
 Serial Number.....A015019764
 Module ID.....0
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)

 Device ID.....97:00.0
 OAM ID.....1
 Serial Number.....A015019708
 Module ID.....4
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)

 Device ID.....2c:00.0
 OAM ID.....2
 Serial Number.....A015019836
 Module ID.....1
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)

 Device ID.....a9:00.0
 OAM ID.....3
 Serial Number.....A015019755
 Module ID.....5
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)

 Device ID.....3d:00.0
 OAM ID.....4
 Serial Number.....A015019768
 Module ID.....2
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)

 Device ID.....ba:00.0
 OAM ID.....5
 Serial Number.....A015019860
 Module ID.....6
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)

 Device ID.....4e:00.0
 OAM ID.....6
 Serial Number.....A015019869
 Module ID.....3
 Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)

 Device ID.....cb:00.0
 OAM ID.....7
```

```
Serial Number.....A015019865
Module ID.....7
Firmware [SPI] Version.....Preboot version hl-gaudi3-1.17.0-fw-
51.0.1-sec-0 (Jun 30 2024 - 00:35:58)

Done
```

### Remote In-Band:

```
saa -I Remote_INB -oi 1.1.1.1 -ou root -op 1234 -c UpdateGpu --dev_id 0 -
-item PVC_UBB_CPLD --file Etron_UBB-SA_CPLD1_A02.jed --remote_saa
root/saa
```

```
SuperServer Automation Assistant 1.0.0 (2023/11/07) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Start to Update firmware of the Habana UBB CPLD
.....
..
Done.
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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
```

### Remote In-Band:

```
saa -I Remote_INB -l SList.txt -c UpdateGpu --dev_id 0 --item
PVC_UBB_CPLD --file Etron_UBB-SA_CPLD1_A02.jed --remote_saa root/saa
```

```
SuperServer Automation Assistant 1.0.0 (2023/11/07) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Start to Update firmware of the Habana UBB CPLD
.....
..
Done.
```

```
SList.txt:
 1.1.1.1 root 1234
 1.1.1.2 root 4321
```

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c UpdateGpu --item
gaudi_spi --file habanalabs-firmware-odm-1.10.0-494.amd64.deb --dev_id
cc:00.0
```

```
SuperServer Automation Assistant 1.0.0 (2023/11/07) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Managed system.....localhost

Unload Habana Driver
.....
.....Gaudi Write Disable Protection Enable

PLEASE DO NOT POWER OFF THE SYSTEM!!!

Gaudi Write Recovery Protection

Show SPI Firmware
.....
.. Device ID.....19:00.0
 OAM ID.....0
 Serial Number.....AM30032493
 Module ID.....2
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

 Device ID.....b3:00.0
 OAM ID.....1
 Serial Number.....AM27043716
 Module ID.....6
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

 Device ID.....cc:00.0
 OAM ID.....3
 Serial Number.....AM30032490
 Module ID.....4
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22)

 Device ID.....43:00.0
 OAM ID.....4
 Serial Number.....AM30032518
 Module ID.....0
 Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
```

---

```
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```
Device ID.....44:00.0
OAM ID.....5
Serial Number.....AM27043781
Module ID.....1
Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
```

```
43.2.0-sec-4 (May 17 2023 - 20:08:22)
```

```
Device ID.....b4:00.0
OAM ID.....7
Serial Number.....AM27043737
Module ID.....7
Firmware [SPI] Version.....Preboot version hl-gaudi2-1.10.0-fw-
43.2.0-sec-4 (May 17 2023 - 20:08:22SList.txt:
```

```
SList.txt:
```

```
1.1.1.1 root 1234
1.1.1.2 root 4321
```

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:

- It is only used for updating NVIDIA HGX A100 8-GPU (Delta), NVIDIA HGX H100/H200 8-GPU (Delta Next), Intel PVC, Intel Gaudi2/3, CG1 MGX and AMD MI300X system firmware. For a comprehensive list of supported platforms and product SKUs, refer to Appendix N. GetGpuInfo/UpdateGpu supported platform matrix.
- This part omits the current FW and ERot version details of FPGA, PCIe Switch, GPU SXMs, NV Switches, PCIe Retimers within the HGX H100 System.
- On the Intel PVC system, igsc must be installed to communicate with the PVC\_IFWI and PVC\_PSCBIN devices.
- On the Intel Gaudi2 system, an additional add-on package (AddOn\_GD2\_Linux\_x86\_64\_YYYYMMDD.tar.gz) should be extracted in the ‘tool’ directory under the SAA installed path, please contact Supermicro for assistance in downloading the add-on package.
- On the Intel Gaudi2/3 system, you must perform a power cycle for Habana driver’s “hl-smi and hl-fw-loader” before updating the gaudi\_spi firmware.

- In the device\_id for gaudi\_spi on the Intel Gaudi2 system, it should be device address, e.g., (cc:00.0).
- Don't need to use dev\_id when using gaudi\_oam\_cpId and gaudi\_spi on the Intel Gaudi3 system.

### 5.12.3. Diagnosing AMD MI250 GPU System Status

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DiagGpuStatus [--dev_id <dev_id_list>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c DiagGpuStatus [-dev_id <dev_id_list>]
Multiple Systems	
OOB	saa -I < system list file > [-u <username> -p <password>] -c DiagGpuStatus [--dev_id <dev_id_list>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DiagGpuStatus
```

The console output contains the following information.

```
AMD INSTINCT MI250
=====
[GPU(1)]
 Serial Number.....PCB012345671
 Power rails Status.....OK
[GPU(2)]
 Serial Number.....PCB012345672
 Power rails Status.....OK
[GPU(3)]
 Serial Number.....PCB012345673
 Power rails Status.....OK
[GPU(4)]
 Serial Number.....PCB012345674
 Power rails Status.....OK
[GPU(5)]
 Serial Number.....PCB012345675
```



---

```
Power rails Status.....OK
[GPU(6)]
Serial Number.....PCB012345676
Power rails Status.....OK
[GPU(7)]
Serial Number.....PCB012345677
Power rails Status.....OK
[GPU(8)]
Serial Number.....PCB012345678
Power rails Status.....OK
```

### **In-Band :**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c DiagGpuStatus --
dev_id 2,4,8
```

**The console output contains the following information.**

```
AMD INSTINCT MI250
=====
[GPU(2)]
Serial Number.....PCB012345672
Power rails Status.....OK
[GPU(4)]
Serial Number.....PCB012345674
Power rails Status.....OK
[GPU(8)]
Serial Number.....PCB012345678
Power rails Status.....OK
```

### **Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DiagGpuStatus
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

---

## 5.12.4. Getting GPU Dump Log Information

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetGpuLog --item <item name> --file <file name> [--overwrite]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetGpuLog --item <item name> --file <file name> [--overwrite]
Multiple Systems	
OOB	saa -I < system list file > [-u <username> -p <password>] -c GetGpuLog --item <item name> --file <file name> [--overwrite]

Example:

### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetGpuLog --item HGX_H100 --file log.tgz
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetGpuLog --item HGX_H100 --type DebugToken --file DebugToken.log
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetGpuLog --item MI300X --file log.tgz
```

### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetGpuLog --item HGX_H100 --file log.tgz
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetGpuLog --item HGX_H100 --type DebugToken --file DebugToken.log
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetGpuLog --item MI300X --file log.tgz
```

**The console output contains the following information for HGX\_H100 and MI300X.**

```
Creating the GPU Log file ...
.....
```

---

```
.....
.....
.....
.....
.....
The GPU Log download file is ready.
File "log.tgz" is created.
```

**The console output contains the following information** for HGX\_H100 Debug Token certificate.

```
Creating the GPU Debug Token Log file ...

Downloading the GPU Debug Token Log file ...
.....
The GPU Log download file is ready.
File "DebugToken.log" is created.
```

#### **Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetGpuLog --item
HGX_H100 --file log.tgz
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetGpuLog --item
HGX_H100 --type DebugToken --file DebugToken.log
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetGpuLog --item
MI300X --file log.tgz
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

If the "Status" field in the execution of the managed system shows SUCCESS, the console output of the managed system will be displayed in the "Execution Message" section of the log file created for the managed system.

## **5.13. CPLD Management**

---

### 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).

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetCpldInfo [--file <filename> [--extract_measurement]]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetCpldInfo [--file <filename> [--file_only] [--extract_measurement]]
Multiple Systems	
OOB	saa -I < system list file > [-u <username> -p <password>] -c GetCpldInfo [--file <filename> [--extract_measurement]]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCpldInfo
```

The console output contains the following information.

```
Managed system.....192.168.34.56
 Motherboard CPLD version.....F1.00.BD
```

#### In-Band:

```
[SAA_HOME]# ./saa -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
 Motherboard CPLD version.....F1.00.BD
 Local CPLD image file.....CPLD.bin
 CPLD version.....F1.00.CD
```

```
FW image.....Signed
Signed Key.....RoT
```

```
[SAA_HOME]# ./saa -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
 Motherboard CPLD version.....F0.09.46
Local CPLD image file.....CPLD.bin
 CPLD version.....F0.0D.5A
 FW image.....Signed
 Signed Key.....RoT

Measurement.....7F3095B7E9ABC6F982719F7A293C68A02373C2BF5C6B7C160D5E
980D90E79708932E6F577B74814C244B81D76F2925F1F456E734CFE67AA8E9CA57C4DA894757
```

**Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -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 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.

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

Type	Descriptions
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.
---------------------	-------------------------------------------------------------------------------------------------------



**Note:**

There could be multiple motherboard CPLD on a single motherboard, their information would be shown with indexed.

### 5.13.2. Updating the CPLD Firmware Image

Use the “UpdateCpld” command with the CPLD firmware image CPLD.bin to run SAA to update the motherboard CPLD of a managed system, and use --index option to specified the CPLD index for the systems with multiple motherboard CPLD supported. The command will update the first motherboard CPLD without --index input.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateCpld --file <filename> [--index <num>] --reboot
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateCpld --file <filename> [--index <num>] --reboot
Multiple Systems	
OOB	saa -I < system list file > [-u <username> -p <password>] -c UpdateCpld --file <filename> [--index <num>] --reboot

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateCpld --file CPLD.bin --reboot
```

**In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateCpld --file CPLD.bin --index 2 --reboot
```

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateCpld --file
CPLD.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.



### Notes:

- This command is only available on X13/H13 and later platforms and X12/H12 RoT systems.
  - The system needs to be powered off while updating the CPLD firmware.
  - This command will update the first motherboard CPLD by default without --index input.
  - DO NOT update CPLD firmware with a wrong index.
- 

### 5.13.3. Getting Switchboard CPLD Firmware Image Information

The command “GetSwitchboardCpldInfo” supports the following features on CPLD RoT systems of X13/H13 and later platforms. Execute the command to get all the switchboards firmware installed on the managed system, but for now, local switchboard firmware image information is not yet supported (with --file\_only option).

Currently, this command is only supported through redfish communication. Hence, in-band command can only be done through the Redfish Host Interface.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSwitchboardCpldInfo
In-Band	saa -l Redfish_HI -u <username> -p <password> -c

	GetSwitchboardCpldInfo
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetSwitchboardCpldInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetSwitchboardCpldInfo
```

**The console output contains the following information** of all switchboards CPLD that can be updated:

```
Managed system.....192.168.34.56
 [Main Switchboard]
 CPLD 1 version.....10
 CPLD 2 version.....0F
 [Left Switchboard]
 CPLD 2 version.....32
 [Right Switchboard]
 CPLD 2 version.....3F
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetSwitchboardCpldInfo
```

```
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.

The switchboard CPLD has the following details:



Type	Description
Main Switchboard	It is possible to install many main switchboards.
Left Switchboard	<i>It is possible to install many left switchboards.</i> Left switchboard only can be displayed if the system has fully boot up.
Right Switchboard	<i>It is possible to install many right switchboards.</i> Right switchboard only can be displayed if the system has fully boot up.



**Notes:**

- Left/Right Switchboard CPLD #1 is not supported for user to get the information.
- Limitation, when the system is in the process of powering up, it is possible for this command to fail. Please wait for the system to fully boot up and then try again.

#### 5.13.4. Updating Switchboard CPLD Firmware Image

The command “UpdateSwitchboardCpld” supports the following features on CPLD RoT systems of X13/H13 and later platforms. Execute the command with Switchboard CPLD image switchboard.jed to update the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateSwitchboardCpld --file <filename> --type <type> [--index <index>] [--reboot]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c UpdateSwitchboardCpld --file <filename> --type <type> [--index <index>] [--reboot]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateSwitchboardCpld --file <filename> --type <type> [--index <index>] [--reboot]

Example:

**00B:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateSwitchboardCpld --file Left_Switchboard_CPLD2.jed --type Left --
index 2
```

The console output displays the following information:

```
Managed system.....192.168.34.56
[Left Switchboard]
CPLD 2 version.....3F

Status: Start updating Switchboard CPLD for 192.168.34.56

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

Uploading FW.....Done

Preparing updating FW.....Done

Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done

Status: Switchboard CPLD is updated for 192.168.34.56

Note: Update done. No further action is needed for this firmware to take effect.
```

## Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
UpdateSwitchboardCpld --file Left_Switchboard_CPLD2.jed --type Left --
index 2
```

```
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.

**Notes:**

- Left/Right Switchboard CPLD #1 is not supported for user to update the firmware.
- Side Switchboard CPLD (Left or Right) firmware can be used interchangeably to update, but not for Main Switchboard as it has its own firmware.
- Reboot option is required when updating the Main Switchboard CPLD, since it can only be updated when the system is in the power off state. Reboot option is optional when updating Side Switchboard CPLD.
- Updating Side Switchboard CPLD requires the system to be in a fully booted up state.
- Limitation, when the system is in the process of powering up, it is possible for this command to fail. Please wait for the system to fully boot up and then try again.

### 5.13.5. Getting Backplane CPLD Firmware Information

Use the “GetBackplaneCpldInfo” command to get the backplane CPLD firmware information from the backplane on managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetBackplaneCpldInfo
In-Band	saa -l Redfish_HI -u <username> -p <password> -c GetBackplaneCpldInfo
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBackplaneCpldInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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 CPLD ID.....0023
 Backplane CPLD Revision.....0C
```

**In-Band Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -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 CPLD ID.....0023
 Backplane CPLD Revision.....0C
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetBackplaneCpldInfo
```

```
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.

### 5.13.6. 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.



**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..>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done
Backplane CPLD ID.....0023
Backplane CPLD Revision.....0C
Local CPLD image file.....BPN_CPLD.jed
Uploading FW...Done
Updating FW..>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done

Status: Backplane CPLD is updated for 192.168.34.56
```

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -c UpdateBackplaneCpld --index 0 --file
BPN_CPLD.jed --manual_ejected
```

```
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.



**Note:**

This command is only available on systems with storage backplanes installed.

---

### 5.13.7. Getting Fanboard CPLD Firmware Image Information

Use the “GetFanboardCpldInfo” command to get the Fanboard CPLD firmware image information of X13/H13 and later RoT platforms from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetFanboardCpldInfo
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetFanboardCpldInfo
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetFanboardCpldInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetFanboardCpldInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
 [Front CPLD]
 Fanboard CPLD 1 version.....01
 [Rear CPLD]
 Fanboard CPLD 1 version.....01
```

**In-Band Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c GetFanboardCpldInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
 [Front CPLD]
 Fanboard CPLD 1 version.....01
```

```
[Rear CPLD]
Fanboard CPLD 1 version.....01
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetFanboardCpldInfo
```

```
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.

The Fanboard CPLD has the following details:

Type	Description
Front Fanboard	The first Fanboard.
Rear Fanboard	The second Fanboard.
Fanboard <num>	The third or above Fanboards.

### 5.13.8. Updating Fanboard CPLD Firmware Image

Use the “UpdateFanboardCpld” command with the Fanboard CPLD firmware image fanboard.jed to run SAA on CPLD RoT systems of X13/H13 and later platforms to update the Fanboard CPLD of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateFanboardCpld --file <filename> --type <Fanboard_ID> [--index <CPLD_ID>]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateFanboardCpld --file <filename> --type <Fanboard_ID> [--index <CPLD_ID>]



Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateFanboardCpld --file <filename> --type <Fanboard_ID> [--index <CPLD_ID>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateFanboardCpld --file Fanboard_CPLD.bin --type Front
```

#### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
UpdateFanboardCpld --file Fanboard_CPLD.bin --type Rear --index 1
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateFanboardCpld
--file Fanboard_CPLD.bin --type Front
```

```
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.

### 5.13.9. Getting AIP CPLD Information

Use the “GetAipCpldInfo” command to get the current AIP (AI Processor) CPLD information from the managed system installed with AIP.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetAipCpldInfo
Multiple Systems	

OOB	saa -l < system list file > [-u <username> -p <password>] -c GetAipCpldInfo
-----	-----------------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetAipCpldInfo
```

```
SList.txt:
 192.168.34.56
```

---

192.168.34.57

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.



**Note:**

This command is supported on the SYS-420GH-TNGR system.

---

### 5.13.10. Updating the AIP CPLD Firmware Image

Use the “UpdateAipCpld” command with the given AIP (AI Processor) CPLD firmware image to run SAA to update the AIP CPLD firmware of managed systems installed with AIP.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateAipCpld --file <filename>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateAipCpld --file <filename>

Example:

**OOB:**

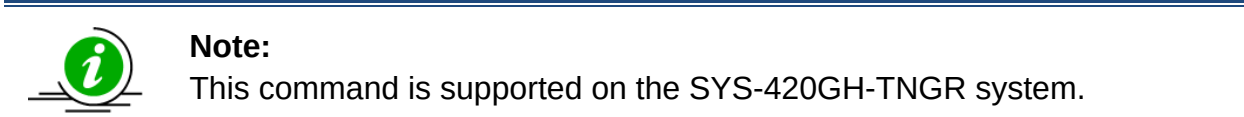
```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateAipCpld --file AIP_CPLD.bin
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateAipCpld --file AIP_CPLD.bin
```

```
SList.txt:
192.168.34.56
```

192.168.34.57



This command is supported on the SYS-420GH-TNGR system.

Example:

**00B:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateAipCpld
--file AIP_CPLD.bin
```

The console output contains the following information.

[illegible]

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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.

### 5.13.11. Getting AOM Board CPLD Firmware Image Information

Use the “GetAomboardCpldInfo” command to get the AOM board CPLD firmware image information of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetAomboardCpldInfo
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetAomboardCpldInfo
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetAomboardCpldInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetAomboardCpldInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
AOM Board CPLD version.....CPLD_ID: 270000D0 Rev: 02
```

**In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c GetAomboardCpldInfo
```

---

The console output contains the following information.

```
Managed system.....169.254.3.254
AOM Board CPLD version.....CPLD_ID: 270000D0 Rev: 02
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetAomboardCpldInfo
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

### 5.13.12. Updating AOM Board CPLD Firmware Image

Use the “UpdateAomboardCpld” command with the AOM board CPLD firmware image AOM\_CPLD.jed to update the AOM board CPLD on the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateAomboardCpld --file <filename> [--dev_id <id>]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateAomboardCpld --file <filename> [--dev_id <id>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateAomboardCpld --file <filename> [--dev_id <id>]

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateAomboardCpld --file AOM_CPLD.jed --dev_id 1
```

#### **In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
UpdateAomboardCpld --file AOM_CPLD.jed
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateAomboardCpld
--file AOM_CPLD.jed
```

```
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.

### **5.13.13. Getting Miscellaneous CPLD Firmware Image Information**

Use the “GetMiscCpldInfo” command to get the motherboard Miscellaneous CPLD firmware image information of NVIDIA MGX™ systems from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetMiscCpldInfo
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetMiscCpldInfo
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetMiscCpldInfo

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetMiscCpldInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
Miscellaneous CPLD version.....0B
```

**In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c GetMiscCpldInfo
```

**The console output contains the following information.**

```
Managed system.....169.254.3.254
Miscellaneous CPLD version.....0B
```

**Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetMiscCpldInfo
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

### 5.13.14. Updating Miscellaneous CPLD Firmware Image

Use the “UpdateMiscCpld” command with the motherboard Miscellaneous CPLD firmware image MISC\_CPLD.jed to run SAA on NVIDIA MGX™ systems to update the Miscellaneous CPLD of a managed system.

<b>Single System</b>
----------------------



OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateMiscCpld --file <filename> --reboot
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateMiscCpld --file <filename> --reboot
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMiscCpld --file <filename> --reboot

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateMiscCpld --file MISC_CPLD.jed --reboot
```

**In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateMiscCpld --file MISC_CPLD.jed --reboot
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateMiscCpld --file MISC_CPLD.jed --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.

### 5.13.15. Getting Midplane SBB CPLD Information

Use the “GetMidplaneSbbCpldInfo” command to get the Midplane Storage Bridge Bay(SBB) CPLD information from the managed system installed directly on the NVMe backplane.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetMidplaneSbbCpldInfo
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetMidplaneSbbCpldInfo
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetMidplaneSbbCpldInfo

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetMidplaneSbbCpldInfo
```

The console output contains the following information.

```
Managed system.....192.168.34.56
 Midplane SBB CPLD 1 version.....CPLD_ID: 0000 REV: 01
```

#### In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c
GetMidplaneSbbCpldInfo
```

The console output contains the following information.

```
Managed system.....169.254.3.254
 Midplane SBB CPLD 1 version.....CPLD_ID: 0000 REV: 01
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetMidplaneSbbCpldInfo
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

If the “Status” field of the managed system shows SUCCESS, the console output will be displayed in the “Execution Message” section of the managed system in the created log file.



**Note:**

This command is supported on systems with Midplane board type.

### 5.13.16. Updating the Midplane SBB CPLD Firmware Image

Use the “UpdateMidplaneSbbCpld” command with the given Midplane Storage Bridge Bay(SBB) CPLD firmware image to run SAA to update the Midplane SBB CPLD firmware of managed systems installed directly on the NVMe backplane.

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c UpdateMidplaneSbbCpld --file &lt;filename&gt; --index &lt;id&gt; --reboot [--post_complete]</code>
Multiple Systems	
OOB	<code>saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c UpdateMidplaneSbbCpld --file &lt;filename&gt; --index &lt;id&gt; --reboot [--post_complete]</code>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateMidplaneSbbCpld --file MidplaneSBB_CPLD.jed --index 1 --reboot --
post_complete
```

**The console output contains the following information.**





**Note:** This command is supported on systems equipped with a Midplane board.

### 5.13.17 Getting NIC CPLD Firmware Image Information

Use the “GetNICCpldInfo” command to get the NIC CPLD firmware image information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetNICCpldInfo
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetNICCpldInfo
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetNICCpldInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetNICCpldInfo
```

**The console output contains the following information.**

```
Managed system..... 192.168.34.56
[NIC 1]
[CPLD 1]
 CPLD Name.....NIC1 CPLD 1 System Slot A1 A0C-A200G-B2CM
 CPLD ID.....32E8
 CPLD Rev.....02
```

**In-Band Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetNICCpldInfo
```

**The console output contains the following information.**

```

Managed system..... 169.254.3.254
 [NIC 1]
 [CPLD 1]
 CPLD Name.....NIC1 CPLD 1 System Slot A1 A0C-A200G-B2CM
 CPLD ID.....32E8
 CPLD Rev.....02

```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetNICCpldInfo
```

```

SList.txt:
 192.168.34.56
 192.168.34.57

```

## 5.13.18 Updating NIC CPLD Firmware Image

Use the “UpdateNICCpld” command with the NIC CPLD firmware image to update NIC CPLD firmware on managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateNICCpld --file <filename> [--dev_id <Device ID>]
In-Band	saa -l Redfish_HI -c UpdateNICCpld --file <filename> [--dev_id <Device ID>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateNICCpld --file <filename> [--dev_id <Device ID>] [--individually]

Example:

### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateNICCpld
--file NIC_CPLD.jed
```

### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateNICCpld --
file NIC_CPLD.jed --dev_id 1_1
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateNICCpld --
file NIC_CPLD.jed
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

**5.13.19. Getting Transitionboard CPLD Information**

Use the “GetTransitionboardCpldInfo” command to get the current Transitionboard CPLD information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetTransitionboardCpldInfo
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetTransitionboardCpldInfo
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetTransitionboardCpldInfo

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetTransitionboardCpldInfo
```

The console output contains the following information.

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

---

```
Transitionboard CPLD Version.....00.00.00
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetTransitionboardCpldInfo
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

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.

## 5.13.20. Updating the Transitionboard CPLD Firmware Image

Use the “UpdateTransitionboardCpld” command with the given Transitionboard CPLD firmware image to update Transitionboard CPLD on managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateTransitionboardCpld --file <filename>
In-Band	saa -I Redfish_HI -c UpdateTransitionboardCpld --file <filename>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateTransitionboardCpld --file <filename>

Example:

### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateTransitionboardCpld --file Transboard_CPLD.jed
```

### In-Band Redfish Host Interface:





```
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.

## 5.14. NIC Management

### 5.14.1. 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).

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetAocNICInfo [--file <filename>] [--dev_id <add-on NIC device ID >]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetAocNICInfo [-file <filename>] [--file_only] [--dev_id <add-on NIC device ID >]
Multiple Systems	
OOB	saa -I < system list file > [-u <username> -p <password>] -c GetAocNICInfo [--file <filename>] [--file_only] [--dev_id <add-on NIC device ID >]

Example:

#### OOB:

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

#### In-Band:

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

## 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:

```
[SAA_HOME]# ./saa -c GetAocNICInfo --file AOC_NIC.bin --file_only
```

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

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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 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.

## 5.14.2. 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateAocNIC [--file <filename> --dev_id <add-on NIC device ID> --reboot] [--post_complete]
In-Band	saa [-l Redfish_HI -u <username> -p <password>] -c UpdateAocNIC {-file <filename> --dev_id <add-on NIC device ID> --reboot}
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateAocNIC [--file <filename> --dev_id <add-on NIC device ID> --reboot] [--post_complete]

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateAocNIC -
-file AOC_NIC.bin --dev_id 1 --reboot --post_complete
```

**In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateAocNIC --
file AOC_NIC.bin --dev_id 1 -reboot
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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.



**Notes:**

- Use the “GetAocNICInfo” command to check the existing device IDs on the managed system.
- For updatable Add-On NIC card chipsets, please refer to the package file, “PlatformFeatureSupportMatrix.pdf” or contact Supermicro technical support.

---

## 5.15. Multi-Node Management

### 5.15.1. Getting TwinPro Settings

Use the “GetTpInfo” command to execute SAA to get the current TwinPro settings from the managed system and save it in the TpInfo.xml file.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetTpInfo [--file <filename> [--overwrite]]
In-Band	saa -c GetTpInfo [--file <filename> [--overwrite]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetTpInfo [--file <filename> [--overwrite]]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetTpInfo --file TpInfo.xml --overwrite
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GetTpInfo --file TpInfo.xml --overwrite
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetTpInfo --file TpInfo.xml --overwrite
```

```
SList.txt:
192.184.11.65
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., TpInfo.xml.192.168.34.56. The --overwrite option is used to force overwrite the existing file, e.g., TpInfo.xml.192.168.34.56.

### 5.15.2. Updating TwinPro Settings

Use the “GetTpInfo” command to execute SAA to get the current TwinPro settings from the managed system and save it in the TpInfo.xml file.

1. Select one managed system as the golden sample for current BMC settings. (For multiple systems usage)
2. Follow the steps in 5.15.1 Getting TwinPro Settings.
3. Edit the configurable element values in the BMC configuration text file TpInfo.xml to the desired values as illustrated in 4.7.7. TwinPro Configuration XML File Format.
4. Skip unchanged tables in the text file by setting the 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.

Use the "ChangeTpInfo" command with the updated TpInfo.xml file to run SAA to update the TwinPro configuration.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChangeTpInfo --file <filename>
In-Band	saa -c ChangeTpInfo --file <filename>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeTpInfo --file <filename> [--individually]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c ChangeTpInfo -
-file TpInfo.xml
```

**In-Band:**

```
./saa -c ChangeTpInfo --file TpInfo.xml
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeTpInfo --
file TpInfo.xml
```

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeTpInfo --
file TpInfo.xml --individually
```

```
SList.txt:
192.184.11.65
192.168.34.57
```

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.

If you want to update 192.168.34.56 and 192.168.34.57, you need to provide two files TpInfo.xml.192.168.34.56 and TpInfo.xml.192.168.34.57. Then set the --file argument with the TpInfo.xml file name. With the --individually option, SAA will search for TpInfo.xml.192.168.34.56 and TpInfo.xml.192.168.34.57 to update 192.168.34.56 and 192.168.34.57, respectively.

### 5.15.3. 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).

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetMultinodeEcInfo [--file <filename>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetMultinodeEcInfo [--file <filename> [--file_only]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetMultinodeEcInfo [--file <filename>]

Example:

**OOB:**



---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetMultinodeEcInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
EC ID.....A7
EC version.....1.20
```

#### **In-Band :**

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetMultinodeEcInfo
```

```
SList.txt:
192.168.34.56
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.

### 5.15.4. Updating the Multi-node EC Firmware Image

Use the “UpdateMultinodeEc” command with the given multi-node EC firmware image EC.bin to run SAA to update the multi-node EC firmware of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateMultinodeEc --file <filename>
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateMultinodeEc --file <filename>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMultinodeEc --file <filename>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateMultinodeEc --file EC.bin
```

**In-Band:**

```
[SAA_HOME]# ./saa -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
```

## Multiple Systems 00B:

```
[SAA_HOME]# ./saa -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 be only run on a system on node A to update EC FW for multi nodes.

## 5.16. VM Management

Use the “GetVmInfo” command to display virtual media information. Use the “VmManage” command with action “Enable” and “Disable” to control virtual media status. For the platforms that support multiple virtual media devices, use the “VmManage” command with action “Mount” and “Unmount” to manage virtual media devices. For the platforms that only support a single virtual media device, use the “MountIsoImage”, “UnMountIsoImage”, “MountFloppyImage” and “UnmountFloppyImage” commands to manage virtual media device.

See the table below for the virtual media features.

Command	SAA	
	Platforms only support single virtual media device	Platforms support multiple virtual media devices
GetVmInfo	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

### 5.16.1. 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. SAA has a rule when using new special characters for virtual media. For more details, see the tables below. 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>&lt;file path> \<hostname or IP>:<port number>&lt;file path> \<hostname or IP>&lt;shared point>&lt;file path> \<hostname or IP>:<port number>&lt;shared point>&lt;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.

Single System	
OoB	saa -i <IP or host name> -u <username> -p <password> -c MountIsoImage --image_url <URL> [--id <id for URL> --pw <password for URL>]   [--id <id for URL> --pw_file <password file path>]]
In-Band	saa [-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>]]
Multiple Systems	
OoB	saa -I <system list file> [-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:

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

---

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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 :**

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

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

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

---

```
[SAA_HOME]# ./saa -c MountIsoImage --image_url
'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbuid --
pw smbpasswd
```

```
[SAA_HOME]# ./saa -c MountIsoImage --image_url
'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbuid --pw
smbpasswd
```

```
[SAA_HOME]# ./saa -c MountIsoImage --image_url
'https://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbuid --
pw smbpasswd
```

```
[SAA_HOME]# ./saa -c MountIsoImage --image_url
'\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id smbuid --pw_file
smbpasswd.txt
```

```
[SAA_HOME]# ./saa -c MountIsoImage --image_url
'\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id smbuid --pw_file
smbpasswd.txt
```

```
smbpasswd.txt:
smbpasswd
```

### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --
image_url 'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id
smbuid --pw smbpasswd
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --
image_url 'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso' --id
smbuid --pw smbpasswd
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --
image_url 'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id
smbuid --pw smbpasswd
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --
image_url 'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id
smbuid --pw smbpasswd
```



---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --
image_url 'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id
smbid --pw smbpasswd
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --
image_url 'https://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --
id smbid --pw smbpassw
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --
image_url '\\192.168.35.1\\MySharedPoint\\MyFolder\\Image.iso' --id smbid --
pw_file smbpasswd.txt
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

```
Smbpasswd.txt:
smbpasswd
```

If the execution “Status” field for a managed system is SUCCESS, the Image.iso is mounted as a virtual media to the managed system.



#### 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 ^ (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.

### 5.16.2. Removing an ISO Image as Virtual Media

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

This command is only supported on platforms that support a single virtual media device only.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UnmountIsoImage
In-Band	saa -u <username> -p <password> -c UnmountIsoImage
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UnmountIsoImage

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UnmountIsoImage
```

#### In-Band:

```
[SAA_HOME]# ./saa -c UnmountIsoImage
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -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.

### 5.16.3. Mounting a Floppy Image as Virtual Media from a Local Image File

Use the “MountFloppyImage” command to have SAA mount a binary floppy image to the managed system virtually. This command is only supported on platforms that support a single virtual media device only.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c MountFloppyImage --file <filename>}
In-Band	saa -c MountFloppyImage --file <filename>}
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c MountFloppyImage --file <filename>}

Example:

#### OOB:

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

#### In-Band:

```
[SAA_HOME]# ./saa -c MountFloppyImage --file Floppy.img
```

The console output will be as below.

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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.
```

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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.



### Note:

The floppy image size should be 1.44 MB.

---

## 5.16.4. Unmounting a Floppy Image as Virtual Media from the Managed System

Use the “UnmountFloppyImage” command to execute SAA to virtually remove a binary floppy image from the managed system. This command is only supported on platforms that support single virtual media device only.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UnmountFloppyImage
In-Band	saa -c UnmountFloppyImage
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UnmountFloppyImage

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UnmountFloppyImage
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c UnmountFloppyImage
```

The console output will be as below.

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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.
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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.

### **5.16.5. Getting Virtual Media Information from the Managed System**

Use the “GetVmInfo” command to get the virtual media information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetVmInfo [--dev_id <device ID>]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c GetVmInfo [--dev_id <device ID>]
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c GetVmInfo [--dev_id <device ID>]
-----	------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetVmInfo
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetVmInfo --
dev_id 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c GetVmInfo
```

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c GetVmInfo --
dev_id 1
```

**The console output contains the following information** if the platform supports managing multiple virtual media devices.

```
SuperServer Automation Assistant 1.0.0 (2023/11/28) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
```

```
Status: Start to get virtual media information.
```

```
Managed system.....192.168.34.56
 Virtual media status.....Enable
 Virtual media port.....623
```

#### Virtual Media Device 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 single virtual media device.

```
SuperServer Automation Assistant 1.0.0 (2023/11/28) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Status: Start to get virtual media information.

Managed system.....192.168.34.56
 Virtual media status.....Enable
 Virtual media port.....623

Virtual Media Device Information
=====
Device 1: Empty device
Device 2: Empty device
Device 3: Empty device
```

**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.

```
SuperServer Automation Assistant 1.0.0 (2023/11/28) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Status: Start to get virtual media information.
```

```
Managed system.....192.168.34.56
 Virtual media status.....Enable
 Virtual media port.....623
```

```
Virtual Media Device Information
=====
Device 1
=====
 Device status: Mounted
 Media type: Floppy
 Connection setting: Applet
 Image: kvm_floppy
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -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.

## 5.16.6. 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 that support virtual media management. For the accepted URL format, please refer to 5.16.1 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, SAA 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, SAA 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, SAA 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.

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c VmManage --action &lt;Enable Disable&gt; [--port &lt;port&gt;] saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c VmManage --action Mount [--dev_id &lt;device ID&gt;] --image_url &lt;URL&gt; [ [--id &lt;id for URL&gt; --pw &lt;password for URL&gt; ][ --id &lt;id for URL&gt; -- pw_file &lt;password file path&gt; ] ] [--verify_cert [--accept_self_signed]] saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c VmManage --action Unmount [--dev_id &lt;device ID&gt;]</pre>
In-Band	<pre>saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c VmManage -- action &lt;Enable Disable&gt; [--port &lt;port&gt;] saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c VmManage -- action Mount [--dev_id &lt;device ID&gt;] --image_url &lt;URL&gt; [ [--id &lt;id for URL&gt; --pw &lt;password for URL&gt; ][ --id &lt;id for URL&gt; --pw_file &lt;password file path&gt; ] ] [--verify_cert [--accept_self_signed]] saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c VmManage -- action Unmount [--dev_id &lt;device ID&gt;]</pre>

Multiple Systems	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c VmManage --action &lt;Enable Disable&gt; [--port &lt;port&gt;] saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c VmManage --action Mount [--dev_id &lt;device ID&gt;] --image_url &lt;URL&gt; [--id &lt;id for URL&gt; --pw &lt;password for URL&gt;][--id &lt;id for URL&gt; --pw_file &lt;password file path&gt;] [--verify_cert [--accept_self_signed]] saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c VmManage --action Unmount [--dev_id &lt;device ID&gt;]</pre>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --
action Enable --port 623
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --
action Disable --port 623
```

```
[SAA_HOME]# ./saa -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 smbuid --pw
smbpasswd --dev_id 1
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --
action Mount --image_url
'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso' --id smbuid --pw
smbpasswd --dev_id 2
```

```
[SAA_HOME]# ./saa -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 smbuid --pw
smbpasswd --dev_id 3
```

```
[SAA_HOME]# ./saa -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 smbuid --
pw_file smbpasswd.txt --dev_id 1
```

---

```
[SAA_HOME]# ./saa -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 smb_id --pw
smbpasswd --verify_cert --accept_self_signed --dev_id 2
```

```
[SAA_HOME]# ./saa -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 smb_id --
pw_file smbpasswd.txt --verify_cert --accept_self_signed --dev_id 3
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --
action Mount --image_url '\\192.168.35.1\MySharedPoint\MyFolder\Image.iso'
--id smb_id --pw_file smbpasswd.txt --dev_id 1
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --
action Mount --image_url '\\2001:db8::1\MySharedPoint\MyFolder\Image.iso'
--id smb_id --pw_file smbpasswd.txt --dev_id 2
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --
action Unmount --dev_id 1
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c VmManage --
action Unmount --dev_id ALL
```

```
smbpasswd.txt:
smbpasswd
```

### **In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Enable --port 623
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Disable --port 623
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' -
-id smb_id --pw smbpasswd --dev_id 1
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso'
```

---

```
--id smbaid --pw smbpasswd --dev_id 2
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso'
--id smbaid --pw smbpasswd --dev_id 3
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url
'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbaid --
pw_file smbpasswd.txt --dev_id 1
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso'
--id smbaid --pw smbpasswd --verify_cert --accept_self_signed --dev_id 2
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url
'https://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbaid --
pw_file smbpasswd.txt --verify_cert --accept_self_signed --dev_id 3
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url '\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id
smbaid --pw_file smbpasswd.txt --dev_id 1
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url '\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id
smbaid --pw_file smbpasswd.txt --dev_id 2
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Unmount --dev_id 1
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c VmManage --action
Unmount --dev_id ALL
```

```
smbpasswd.txt:
smbpasswd
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Enable --port 623
```

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Disable --port 623
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' -
-id sbmid --pw smbpasswd --dev_id 1
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'smb://[2001:db8::1]/MySharedPoint/MyFolder/Image.iso'
--id sbmid --pw smbpasswd --dev_id 2
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'http://192.168.35.1/MySharedPoint/MyFolder/Image.iso'
--id sbmid --pw smbpasswd --dev_id 3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url
'http://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id sbmid --
pw_file smbpasswd.txt --dev_id 1
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url 'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso'
--id sbmid --pw smbpasswd --verify_cert --accept_self_signed --dev_id 2
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url
'https://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id sbmid --
pw_file smbpasswd.txt --verify_cert --accept_self_signed --dev_id 3
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url '\\192.168.35.1\MySharedPoint\MyFolder\Image.iso' --id
sbmid --pw_file smbpasswd.txt --dev_id 1
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Mount --image_url '\\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id
sbmid --pw_file smbpasswd.txt --dev_id 2
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Unmount --dev_id 1
```

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c VmManage --action
Unmount --dev_id ALL
```

```
smbpasswd.txt:
smbpasswd
```

```
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:**

- 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 ^ (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.
- 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.

---

### 5.16.7. Managing Virtual Media Devices in SAA Shell Mode

Use the “VMShell” command to manage the Virtual Media Devices for the managed system under SAA shell mode. Before running "VMShell" command, you need to enter SAA shell mode, refer to 5.11.11. Shell Mode for details See below for details on using VMShell.

- **For the devlist Action:**  
Use the “--action devlist” option to list the available devices that can be mounted to the virtual media device 1 of BMC.
  - Hard drives can be listed but can not be mounted due to OS security concerns.
- **For the dev1drv Action:**  
Use the “--action dev1drv” option to mount a local USB device to the virtual media device 1 of BMC.
  - Use the --index option to specify the index of the local USB device.
- **For the dev2iso Action:**  
Use the “--action dev2iso” option to mount a local ISO image file to the virtual media device 2 of BMC.
  - Use the --file option to specify the local ISO image file.
- **For the dev1stop/dev2stop Action:**  
Use the “--action dev1stop/dev2stop” option to stop the virtual media device 1/2 of the BMC.
- **For the status Action:**  
Use the “--action status” option to show the status virtual media devices of BMC.
  - Use the --dev\_id option to specify the device ID of the specified device.
  - Without the --dev\_id option, status for all virtual media devices will be listed.
- **For the log Action:**  
Use the “--action log” option to show the history of actions for the virtual media devices of the BMC.

Single System	
SAA shell	VMShell --action <action> [--index <index>] [--file <file name>] [--dev_id <Device ID>]

---

Example:

**SAA shell:**

```
[SAA_HOME]# X12_ATEN_AST2600> VMShell --action devlist
```

**The console output contains the following information** if the platform supports managing multiple virtual media devices.

```
.....
3: [sdc1: SCSI Disk]
4: [sdd1: SCSI Disk]
5: [sda1: SCSI Disk]
6: [sdb1: SCSI Disk]
```

```
[SAA_HOME]# X12_ATEN_AST2600> VMShell --action dec1drv --index 3
```

**The console output contains the following information**

```
.....
Mounting sdc1: SCSI Disk...
Device 1 : VM Plug-In OK!!
```

```
[SAA_HOME]# X12_ATEN_AST2600> VMShell --action dec2iso --file
efishell.iso
```

**The console output contains the following information**

```
.....
Mounting ISO file: efishell.iso.....
Device 2 : VM Plug-In OK!!
```

```
[SAA_HOME]# X12_ATEN_AST2600> VMShell --action dev1stop
```

**The console output contains the following information**

```
.....
Device 1 : VM Plug-Out OK!! Stop!!
```



---

```
[SAA_HOME]# X12_ATEN_AST2600> VMShell --action log
```

**The console output contains the following information**

```
Device 1 : VM Plug-In OK!!
Device 2 : VM Plug-In OK!!
Device 1 : VM Plug-Out OK!! Stop!!
```

```
[SAA_HOME]# X12_ATEN_AST2600> VMShell --action status
```

**The console output contains the following information** if the platform supports managing multiple virtual media devices.

```
.....
Status: Start to get virtual media information.

Managed system.....192.168.34.56
 Virtual media status.....Enable
 Virtual media port.....623

Virtual Media Device Information
=====
```

Device 1
=====
Device status: Mounted
Media type: USBStick
Connection setting: Applet
Image: kvm_usb

Device 2
=====
Device status: Mounted
Media type: CD/DVD
Connection setting: Applet
Image: kvm_cd

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 single virtual media device.

```
.....
Status: Start to get virtual media information.

Managed system.....192.168.34.56
 Virtual media status.....Enable
 Virtual media port.....623

Virtual Media Device Information
=====
 Device 1: Empty device
 Device 2: Disk Device
 Device 3: Empty device
```

```
[SAA_HOME]# X12_ATEN_AST2600> VMShell --action status --dev_id 1
```

**The console output contains the following information**

```
.....
Status: Start to get virtual media information.

Managed system.....192.168.34.56
 Virtual media status.....Enable
 Virtual media port.....623

Virtual Media Device Information
=====
 Device 1
 =====
 Device status: Mounted
 Media type: USBStick
 Connection setting: Applet
 Image: kvm_usb
```

## 5.17. NM Management

### 5.17.1. Managing Intel Management Engine

The NmMeManage command can manage the Intel management engine (ME) through Intel Intelligent Power Node Manager for Supermicro Intel platforms.

The following table summarizes the supported actions in the NmMeManage command for each Intel Node Manager version.

Option	--type	--action
<b>Description</b>	NM20 = Node manager 2.0	GetDeviceID = Get ME device ID Reset = Reboots ME ResetToDefault = Resets ME to default EnterToUpdateMode = Forces ME to update mode PowerOff = Sets ME power state off SelfTest = Gets self-test results Mode = Gets ME running mode ListImagesInfo = Lists ME images information GetPower = Gets power information from ME GetTemp = Gets temperature information from ME



**Note:**

- Starting from X14 and later platforms, the NmMeManage command is not supported since these platforms do not have Management Engine (ME) to support Intel node manager management.

The following chapters will describe each action in detail.

#### 5.17.1.1. Getting ME Device ID

Use the NmMeManage command with option --action GetDeviceID to get the ME device ID from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action GetDeviceID
In-Band	saa -c NmMeManage --type NM20 --action GetDeviceID
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action GetDeviceID

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --
type NM20 --action GetDeviceID
```

**In-Band:**

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action GetDeviceID
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type
NM20 --action GetDeviceID
```

```
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.

### 5.17.1.2. Resetting ME

Use the NmMeManage command with option --action Reset to reboot ME from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action Reset
In-Band	saa -c NmMeManage --type NM20 --action Reset
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action Reset

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --
type NM20 --action Reset
```

**In-Band:**

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action Reset
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type
NM20 --action Reset
```

```
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.

### 5.17.1.3. Resetting ME to Default

Use the NmMeManage command with option --action ResetToDefault to force ME reset to default settings from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action ResetToDefault
In-Band	saa -c NmMeManage --type NM20 --action ResetToDefault
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action ResetToDefault

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --
type NM20 --action ResetToDefault
```

**In-Band:**

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action ResetToDefault
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type
NM20 --action ResetToDefault
```

```
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.

#### 5.17.1.4. Entering To Update Mode

Use the NmMeManage command with option --action EnterToUpdateMode to force ME to enter the update mode from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action EnterToUpdateMode
In-Band	saa -c NmMeManage --type NM20 --action EnterToUpdateMode
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action EnterToUpdateMode

---

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --
type NM20 --action EnterToUpdateMode
```

**In-Band:**

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action EnterToUpdateMode
```

**Multiple OoB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type
NM20 --action EnterToUpdateMode
```

```
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.

### 5.17.1.5. Powering Off ME

Use the NmMeManage command with option --action PowerOff to set ME to the power-off state from managed system.

Please note that if the BMC status is S0/S1, you cannot turn off ME immediately. It will display a “not support in present state” message. To power off ME, you should turn off the chassis power first.

Single System	
OoB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action PowerOff
In-Band	saa -c NmMeManage --type NM20 --action PowerOff
Multiple Systems	

OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c NmMeManage --type NM20 --action PowerOff</code>
-----	------------------------------------------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action PowerOff
```

#### In-Band:

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action PowerOff
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action PowerOff
```

```
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.

#### 5.17.1.6. Self-Test

Use the NmMeManage command with option --action SelfTest to get the self-test results from managed system.

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c NmMeManage --type NM20 --action SelfTest</code>
In-Band	<code>saa -c NmMeManage --type NM20 --action SelfTest</code>
Multiple Systems	



OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action SelfTest
-----	-----------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action SelfTest
```

#### In-Band:

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action SelfTest
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action SelfTest
```

```
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.

#### 5.17.1.7. Getting ME Mode

Use the NmMeManage command with option --action Mode to get the ME running mode from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action Mode
In-Band	saa -c NmMeManage --type NM20 --action Mode
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action Mode
-----	-------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action Mode
```

#### In-Band:

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action Mode
```

The console output contains the following information.

```
ME is in NORMAL mode.
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action Mode
```

```
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.

#### 5.17.1.8. Listing ME Images Information

Use the NmMeManage command with option --action ListImagesInfo to get the information of ME images from managed system.

#### Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action ListImagesInfo
In-Band	saa -c NmMeManage --type NM20 --action ListImagesInfo
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action ListImagesInfo

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action ListImagesInfo
```

#### In-Band:

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action ListImagesInfo
```

The console output contains the following information.

```
Recovery Image:
Image Type = recovery image
raw = 57 01 00 02 01 02 07 35 00

1st operational Image:
Image Type = operational image 1 (This Image is currently running)
raw = 57 01 00 02 01 02 07 35 05

2nd operational Image:
Image Type = operational image 2
raw = 57 01 00 02 01 02 07 35 02
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action ListImagesInfo
```

```
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.

#### 5.17.1.9. Getting Power Information from ME

Use the NmMeManage command with option --action GetPower to get power information from ME of managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action GetPower
In-Band	saa -c NmMeManage --type NM20 --action GetPower
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action GetPower

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action GetPower
```

##### In-Band:

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action GetPower
```

The console output contains the following information.

```
56 watts
```

##### Multiple OOB:

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action GetPower
```

```
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.

#### 5.17.1.10. Getting Temperature Information from ME

Use the NmMeManage command with the --action GetTemp option to get the temperature information from ME of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action GetTemp
In-Band	saa -c NmMeManage --type NM20 --action GetTemp
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action GetTemp

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmMeManage --type NM20 --action GetTemp
```

##### In-Band:

```
[SAA_HOME]# ./saa -c NmMeManage --type NM20 --action GetTemp
```

The console output contains the following information.

---

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmMeManage --type
NM20 --action GetTemp
```

```
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.

### 5.17.2. Managing Node Manager

The GeneralNmManage command can manage a node manager by Intel Intelligent Power Node Manager (NM) or BMC Intel Node Manager (BMC-NM) for Supermicro Intel platforms

The following table summarizes the supported actions in the GeneralNmManage command for each NM or BMC-NM version.

Option	--type	--action
Description	NM20 = Node manager 2.0	GetNMSSDR = Displays NM sensor data record GetSelTime = Gets system event log time GetStatistics = Gets NM statistics ResetStatistics = Resets NM statistics GetCapabilities = Gets NM capabilities GetVersion = Gets NM version GetAlert = Gets NM alert SetAlert = Sets NM alert GetTotalPower = Gets total power budget SetTotalPower = Sets total power budget DelTotalPower = Deletes total power budget SetPowerDrawRange = Sets NM power draw range

		GetSensor = Gets sensor data GetSummary = Gets NM summary information
	BMC10 = BMC Intel Node Manager 1.0	GetSelTime = Gets system event log time GetStatistics = Gets NM statistics ResetStatistics = Resets NM statistics GetCapabilities = Gets NM capabilities GetVersion = Gets NM version GetTotalPower = Gets total power budget SetTotalPower = Sets total power budget DelTotalPower = Deletes total power budget SetPowerDrawRange = Sets NM power draw range GetSummary = Gets NM summary information



**Notes:**

- Starting from X14 and later platforms, please use the --type BMC10 option instead of NM20. These platforms do not have Management Engine (ME) to support Intel node manager management.

The following chapters will describe each action in detail.

### 5.17.2.1. Managing Node Manager by Intel Intelligent Power Node Manager

#### 5.17.2.1.1. Getting Blade Power Supply Unit Information

Use the GeneralNmManage command with option --action GetNMSDR to get the node manager sensor data record (SDR) from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetNMSDR
In-Band	saa -c GeneralNmManage --type NM20 --action GetNMSDR
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetNMSDR

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action GetNMSDR
```

**In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action GetNMSDR
```

**The console output contains the following information.**

```
Record ID = 1C 00
SDR Version = 51h
Record Type = C0h
Record Length = 0Bh
OEM ID = 57 01 00 h
Record Subtype = 0Dh
SubType Version = 01h
Slave Address = 2Ch
Channel = 00h
Health Event Sensor Number = 1Dh
Exception Event Sensor Number = 1Eh
Operational Capabilities Sensor Number = 1Fh
Alert Threshold Exceeded Sensor Number = 20h
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action GetNMSDR
```

```
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.

### 5.17.2.1.2. Getting System Event Log Time



---

Use the GeneralNmManage command with option --action GetSelTime to get system event log (SEL) time from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetSelTime
In-Band	saa -c GeneralNmManage --type NM20 --action GetSelTime
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetSelTime

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action GetSelTime
```

**In-Band:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action GetSelTime
```

**The console output contains the following information.**

```
SEL Time = 2023/08/25 08:38:02
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action GetSelTime
```

```
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.

### 5.17.2.1.3. Getting Node Manager Statistics

Use the GeneralNmManage command with option --action GetStatistics to get node manager (NM) statistics from managed system.

The following are the supported options for option --action GetStatistics.

Option	Description
--mode	1(01h): Global power statistics in [Watts] 2(02h): Global inlet temperature statistics in [Celsius] 3(03h): Global throttling statistics [%] (NM 3.0) 4(04h): Global volumetric airflow statistics [1/10th of CFM] (NM 3.0) 5(05h): Global outlet airflow temperature statistics [Celsius] (NM 3.0) 6(06h): Global chassis power statistics [Watts] (NM 3.0) 17(11h): Per policy power statistics in [Watts] 18(12h): Per policy trigger statistics in [Celsius] 19(13h): Per policy throttling statistics in [%] (NM 3.0) 27(1Bh): Global Host Unhandled Requests statistics 28(1Ch): Global Host Response Time statistics 29(1Dh): Global CPU throttling statistics 30(1Eh): Global memory throttling statistics 31(1Fh): Global Host Communication Failure statistics
--policy_id	Apply for mode 11h or 12h. Otherwise, set to 0.
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection (NM 3.0) 4: High Power I/O subsystem For mode in a range 1Bh to 1Fh Domain ID must be set to 00h.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>

In-Band	saa -c GeneralNmManage --type NM20 --action GetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action GetStatistics --mode 1 --domain_id 0
--policy_id 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action GetStatistics --mode 1 --domain_id 0 --policy_id 0
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action GetStatistics --mode 1 --domain_id 0 --policy_id 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.

#### 5.17.2.1.4. Resetting Node Manager Statistics

Use the GeneralNmManage command with option --action ResetStatistics to reset node manager (NM) statistics from managed system.

The following are the supported options for option --action ResetStatistics.

Option	Description
--mode	1(01h): Global power statistics in [Watts] 2(02h): Global inlet temperature statistics in [Celsius] 27(1Bh): Global Host Unhandled Requests statistics 28(1Ch): Global Host Response Time statistics 29(1Dh): Global CPU throttling statistics 30(1Eh): Global memory throttling statistics 31(1Fh): Global Host Communication Failure statistics
--policy_id	Policy ID will be ignored if mode is 0h. Otherwise, set to 0.
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection (NM 3.0) 4: High Power I/O subsystem For mode in a range 1Bh to 1Fh Domain ID must be set to 00h.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>
In-Band	saa -c GeneralNmManage --type NM20 --action ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action ResetStatistics --mode 0 --domain_id
0 --policy_id 0
```

#### In-Band:

---

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action ResetStatistics --mode 0 --domain_id 0 --policy_id 0
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action ResetStatistics --mode 0 --domain_id 0 --policy_id 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.

#### 5.17.2.1.5. Getting Node Manager Capabilities

Use the GeneralNmManage command with option --action GetCapabilities to get node manager (NM) capabilities from managed system.

The following are the supported options for option --action GetCapabilities.

Option	Description
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection (NM 3.0) 4: High Power I/O subsystem For mode in a range 1Bh to 1Fh Domain ID must be set to 00h.
--trigger_type	0: No Policy Trigger 1: Inlet Temperature Policy Trigger value in [Celsius] 2: Missing Power Reading Timeout in 1/10th of second 3: Time After Host Reset Trigger in 1/10th of second 4: Boot time policy 6: MGPIO Policy Trigger

### Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type>
In-Band	saa -c GeneralNmManage --type NM20 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type>
<b>Multiple Systems</b>	
OOB	saa -I <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action GetCapabilities --domain_id 0 --
trigger_type 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action GetCapabilities --domain_id 0 --trigger_type 0
```

The console output contains the following information.

```
Max concurrent settings = 16
Max Power/Thermal/Time After Reset = 32767
Min Power/Thermal/Time After Reset = 1
Max Correction Time settable = 600000 ms
Min Correction Time settable = 3000 ms
Max Statistics Reporting period = 3600 s
Min Statistics Reporting period = 1 s
Domain ID:
 Entire platform
Limiting based on:
 DC power - PSU output power or bladed system
raw = 57 01 00 10 FF 7F 01 00 B8 0B 00 00 C0 27 09 00 01 00 10 0E 00
```

#### Multiple OOB:

---

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --type NM20 --action GetCapabilities --domain_id 0 --trigger_type 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.

#### 5.17.2.1.6. Getting Node Manager Version

Use the GeneralNmManage command with option --action GetVersion to show node manager (NM) version from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetVersion
In-Band	saa -c GeneralNmManage --type NM20 --action GetVersion
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetVersion

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GeneralNmManage --type NM20 --action GetVersion
```

##### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage --type NM20 --action GetVersion
```

The console output contains the following information.

---

```
Node Manager Version = 2.0
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action GetVersion
```

```
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.

#### 5.17.2.1.7. Getting Node Manager Alert

Use the GeneralNmManage command with option --action GetAlert to get node manager (NM) alert from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetAlert
In-Band	saa -c GeneralNmManage --type NM20 --action GetAlert
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetAlert

Example:

### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action GetAlert
```

### In-Band:



```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action GetAlert
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action GetAlert
```

```
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.

#### 5.17.2.1.8. Setting Node Manager Alert

Use the GeneralNmManage command with option --action SetAlert to set node manager (NM) alert from managed system.

The following is the supported option for option --action SetAlert.

Option	Description
--value	Specifies SNMP sequence from 1 to 15. Check SNMP sequence by SnmpManage command.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action SetAlert --value <assignment value>
In-Band	saa -c GeneralNmManage --type NM20 --action SetAlert --value <assignment value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action SetAlert --value <assignment

	value>
--	--------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action SetAlert --value 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action SetAlert --value 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action SetAlert --value 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.

#### 5.17.2.1.9. Getting Total Power Budget

Use the GeneralNmManage command with option --action GetTotalPower to get total power budget from managed system.

The following is the supported option for option --action GetTotalPower.

Option	Description
--domain_id	0: Entire platform 1: CPU subsystem

	2: Memory subsystem 4: High Power I/O subsystem
--	----------------------------------------------------

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetTotalPower --domain_id <Domain ID>
In-Band	saa -c GeneralNmManage --type NM20 --action GetTotalPower --domain_id <Domain ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetTotalPower --domain_id <Domain ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action GetTotalPower --domain_id 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action GetTotalPower --domain_id 0
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action GetTotalPower --domain_id 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.

#### 5.17.2.1.10. Setting Total Power Budget

Use the GeneralNmManage command with option --action SetTotalPower to set total power budget from managed system.

The following are the supported options for option --action SetTotalPower.

Option	Description
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem
--value	Assigns watt for total power budget.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action SetTotalPower --domain_id <Domain ID> --value <assignment value>
In-Band	saa -c GeneralNmManage --type NM20 --action SetTotalPower -- domain_id <Domain ID> --value <assignment value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action SetTotalPower --domain_id <Domain ID> --value <assignment value>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action SetTotalPower --domain_id 0 --value
100
```

#### In-Band:

---

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action SetTotalPower --domain_id 0 --value 100
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action SetTotalPower --domain_id 0 --value 100
```

```
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.

#### 5.17.2.1.11. Deleting Total Power Budget

Use the GeneralNmManage command with option --action DelTotalPower to delete total power budget from managed system.

The following is the supported option for option --action DelTotalPower.

Option	Description
--domain_id	0: Entire platform 1: CPU subsystem 2: Memory subsystem 4: High Power I/O subsystem

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action DelTotalPower --domain_id <Domain ID>
In-Band	saa -c GeneralNmManage --type NM20 --action DelTotalPower -- domain_id <Domain ID>
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action DelTotalPower --domain_id <Domain ID>
-----	---------------------------------------------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action DelTotalPower --domain_id 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GeneralNmManage --type NM20 --action DelTotalPower -
-domain_id 0
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action DelTotalPower --domain_id 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.

#### 5.17.2.1.12. Setting Power Draw Range

Use the GeneralNmManage command with option --action SetPowerDrawRange to set the node manager (NM) power draw range from managed system.

The following are the supported options for option --action SetPowerDrawRange.

Option	Description
--domain_id	0: Entire platform 1: CPU subsystem

	2: Memory subsystem 4: High Power I/O subsystem
--range	Specifies power draw range. Power draw range: 0-32767

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range>
In-Band	saa -c GeneralNmManage --type NM20 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action SetPowerDrawRange --domain_id 0 --
range 0-32767
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action SetPowerDrawRange --domain_id 0 --range 0-32767
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action SetPowerDrawRange --domain_id 0 --range 0-32767
```

```
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.

#### 5.17.2.1.13. Getting Sensor Data

Use the GeneralNmManage command with option --action GetSensor to get the sensor data of node manager from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetSensor
In-Band	saa -c GeneralNmManage --type NM20 --action GetSensor
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetSensor

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action GetSensor
```

##### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action GetSensor
```

The console output contains the following information.

```
| Id | Sensor | Reading | Low Limit | High
Limit |
| -----|-----
-----|
| 8 | PCH Thermal Threshold | 43C/109F | 2C/36F |
```



```

95C/203F |
| 32 | CPU 0 Thermal Control Circuit Activation | 0 % | 0 % | 0 %
|
| 52 | CPU 0 Memory Throttling | 0 % | 0 % | 0 %
|
| 163 | Inlet Airflow Temperature | 36C/97F | 0C/32F |
247C/477F |
| 173 | Total Chassis power | 4 W | 0 W | 0 W
|
| 190 | Core CUPS | 0 % | N/A | N/A
|
| 191 | IO CUPS | 0 % | N/A | N/A
|
| 192 | Memory CUPS | 0 % | N/A | N/A
|
| ----- | ----- | ----- | -----
--- |
| 28 | CPU 0 Thermal Status | Normal |
| 36 | CPU 0 T-Control | 8 |
| 48 | CPU 0 T-JMAX | 93 |

```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action GetSensor
```

```

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.

#### 5.17.2.1.14. Getting Node Manager Summary Information

Use the GeneralNmManage command with option --action GetSummary to get the summary information of node manager (NM) from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type NM20 --action GetSummary

In-Band	saa -c GeneralNmManage --type NM20 --action GetSummary
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetSummary

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type NM20 --action GetSummary
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type NM20 --action GetSummary
```

**The console output contains the following information.**

```

Intel Intelligent Power Node Manager 6.0 (6.0.4.70)
SEL Time - 2023/08/25 09:57:53
Node Manager Policy: Not set
Total Power Budget: Not set
DCMI Power Limit: Disabled or not set
CUPS Policy: Not set
CPU Information
+-----+
| P-State| T-State| Max Allowed Cores|
+-----+
| 0/16| 0/1| 32/32|
+-----+
Power Usage
+-----+
|Domain | Usage (W)|
+-----+
|Entire platform | 114|
+-----+
|CPU subsystem | 0|
+-----+
|Memory subsystem | 4|
+-----+
CUPS Utilization
+-----+
|Domain | Usage (%)|
+-----+

```

```
|Core | 0|
+-----+
|Memory | 0|
+-----+
|IO | 0|
+-----+
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type NM20 --action GetSummary
```

```
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.

### 5.17.2.2. Managing Node Manager by BMC Intel Node Manager

When managing the Node Manager by the BMC Intel Node Manager, some domain management requires Power into System (Psys) support. For the usage of the PowerPolicy command with the --type BMC10 (BMC Intel Node Manager 1.0) option, the --domain\_id option with 0 (Entire platform, AC power), 4 (PCIe devices subsystem) or 5 (Entire platform, DC power) requires Psys support.

#### 5.17.2.2.1. Getting System Event Log Time

Use the GeneralNmManage command with the --action GetSelTime option to get the system event log (SEL) time from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action GetSelTime
In-Band	saa -c GeneralNmManage --type BMC10 --action GetSelTime

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action GetSelTime

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action GetSelTime
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GeneralNmManage --type BMC10 --action GetSelTime
```

The console output contains the following information.

```
SEL Time = 2024/04/03 06:50:30
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action GetSelTime
```

```
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.

#### 5.17.2.2.2. Getting BMC Intel Node Manager Statistics

Use the GeneralNmManage command with the --action GetStatistics option to get BMC Intel Node Manager statistics from the managed system.

The following options are supported for the --action GetStatistics option.

Option	Description
--mode	1(01h): Global power statistics in [Watts] 2(02h): Global inlet temperature statistics in [Celsius] 3(03h): Global throttling statistics [%] 4(04h): Global volumetric airflow statistics [1/10th of CFM] 5(05h): Global outlet airflow temperature statistics [Celsius] 6(06h): Global chassis power statistics [Watts] 17(11h): Per policy power statistics in [Watts] 18(12h): Per policy trigger statistics in [Celsius] 29(1Dh): Global CPU throttling statistics (deprecated, Mode=03h, Domain ID=01h should be used instead) 30(1Eh): Global memory throttling statistics (deprecated, Mode=03h, Domain ID=02h should be used instead)
--policy_id	Apply for mode 11h or 13h. Otherwise, set to 0.
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required) For mode in a range 1Bh to 1Fh Domain ID must be set to 00h.
--per_component_control	Allows for getting data for chosen domain component. 0 - Accumulated data for whole domain will be returned. 1 - Data from single component in domain will be returned.
--component_id	Apply for mode 01h, 08h and Per-component Control = 1. <ol style="list-style-type: none"> <li>For the CPU Domain, the component identifier is the CPU socket number (0–7). where 0 refers to the lowest numbered address on the PECE bus.</li> <li>For the Memory Domain, the component identifier is the CPU socket number (0–7). where 0 refers to the lowest numbered address on the PECE bus associated with the memory channels.</li> <li>For the PCIe Domain, the component identifier is the PCIe card index.</li> </ol>

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action GetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> --

	per_component_control <Per-component Control> --component_id <Component ID>
In-Band	saa -c GeneralNmManage --type BMC10 --action GetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> --per_component_control <Per-component Control> --component_id <Component ID>
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action GetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> --per_component_control <Per-component Control> --component_id <Component ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action GetStatistics --mode 1 --domain_id
1 --policy_id 1 --per_component_control 0 --component_id 0
```

The console output contains the following information.

```
Current = 66 w
Minimum = 0 w
Maximum = 72 w
Average = 67 w
Time = 2024/04/08 03:55:25
Reporting Period = 384609 sec
Domain ID:
 CPU subsystem
Policy/Global Administrative state:
 NM Policy Control is Globally Enabled
Measurements state:
 Measurements in progress
raw = 57 01 00 42 00 00 00 48 00 43 00 AD 6A 13 66 61 DE 05 00 51
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action GetStatistics --mode 2 --domain_id
2 --policy_id 0 --per_component_control 1 --component_id 0
```

#### In-Band:

---

```
[SAA_HOME]# ./saa -c GeneralNmManage --type BMC10 --action GetStatistics
--mode 1 --domain_id 1 --policy_id 1 --per_component_control 0 --
component_id 0
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action GetStatistics --mode 1 --domain_id 1 --policy_id 1 --
per_component_control 0 --component_id 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.

#### 5.17.2.2.3. Resetting BMC Intel Node Manager Statistics

Use the GeneralNmManage command with the --action ResetStatistics option to reset the BMC Intel Node Manager statistics from the managed system.

The following options are supported for the --action ResetStatistics option.

Option	Description
--mode	0(00h): global statistics including power and inlet temp 1(01h): per policy statistics including power and trigger statistics 27(1Bh): global Host Unhandled Requests statistics 28(1Ch): global Host Response Time statistics 29(1Dh): global CPU throttling statistics (deprecated) 30(1Eh): global memory throttling statistics (deprecated) 31(1Fh): global Host Communication Failure statistics
--policy_id	Policy ID will be ignored if mode is 1h. Otherwise, set to 0.
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem

	4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)
--	-----------------------------------------------------------------------------------------------------------------

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>
In-Band	saa -c GeneralNmManage --type BMC10 --action ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action ResetStatistics --mode 1 --
domain_id 1 --policy_id 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type BMC10 --action ResetStatistics --mode 1 --domain_id 1 --policy_id 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action ResetStatistics --mode 1 --domain_id 1 --policy_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.

#### 5.17.2.2.4. Getting BMC Intel Node Manager Capabilities

Use the GeneralNmManage command with the --action GetCapabilities option to get the BMC Intel Node Manager capabilities from the managed system.

The following options are supported for the --action GetCapabilities option.

Option	Description
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)
--trigger_type	0: No Policy Trigger 1: Inlet Temperature Policy Trigger value in [Celsius] 2: Missing Power Reading Timeout in 1/10th of second 3: Time After Host Reset Trigger in 1/10th of second 6: GPIO Policy Trigger 7: C0 Residency in [%]. Activated after average C0 residency calculated over Correction Time falls below value in Trigger Limit. 8: Host Reset. Activated when host reset occurs, deactivated on End of POST event. 9: SMBAlert Interrupt. Activated when SMBAlert# interrupt is detected.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type>
In-Band	saa -c GeneralNmManage --type BMC10 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action GetCapabilities --

	domain_id <Domain ID> --trigger_type <Trigger Type>
--	-----------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action GetCapabilities --domain_id 1 --
trigger_type 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -c GeneralNmManage --type BMC10 --action
GetCapabilities --domain_id 1 --trigger_type 0
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action GetCapabilities --domain_id 0 --trigger_type 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.

#### 5.17.2.2.5. Getting BMC Intel Node Manager Version

Use the GeneralNmManage command with the --action GetVersion option to show the version of BMC Intel Node Manager from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action GetVersion
In-Band	saa -c GeneralNmManage --type BMC10 --action GetVersion
Multiple Systems	

OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c GeneralNmManage --type BMC10 --action GetVersion</code>
-----	--------------------------------------------------------------------------------------------------------------------------------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action GetVersion
```

The console output contains the following information.

```
BMC Intel Node Manager = 1.0
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type BMC10 --action GetVersion
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action GetVersion
```

```
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.

#### 5.17.2.2.6. Getting Total Power Budget

Use the GeneralNmManage command with the --action GetTotalPower option to get the total power budget from the managed system..

The following option is supported for the --action GetTotalPower option.

Option	Description
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)
-- per_component_control	Allows for setting the power budget for chosen domain component. 1 - Power budget should be applied to given component in domain (volatile setting).
--component_id	If the Per Component Control flag is set, this field contains component identifier for which power budget should be returned. Otherwise, the value in this field is ignored.  1. For the CPU Domain, the component identifier is the CPU socket number (0–7) where 0 refers to the lowest numbered address on the PECE bus. 2. For the Memory Domain, the component identifier is the CPU socket number (0–7) where 0 refers to the lowest numbered address on the PECE bus associated with the memory channels. 3. For the PCIe Domain, the component identifier is the PCIe card index.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action GetTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID>
In-Band	saa -c GeneralNmManage --type BMC10 --action GetTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action GetTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID>

Example:

---

## OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action GetTotalPower --domain_id 0 --
per_component_control 1 --component_id 0
```

The console output contains the following information.

```
Total Power Budget in [Watts] = 100
```

## In-Band:

```
[SAA_HOME]# ./saa -c GeneralNmManage --type BMC10 --action GetTotalPower
--domain_id 0 --per_component_control 1 --component_id 0
```

## Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action GetTotalPower --domain_id 0 --per_component_control 1
--component_id 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.

### 5.17.2.2.7. Setting Total Power Budget

Use the GeneralNmManage command with the --action SetTotalPower option to set the total power budget from the managed system.

The following options are supported for the --action SetTotalPower option.

Option	Description
--value	Assigns watt for total power budget.

--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)
-- per_component_control	Allows for setting the power budget for chosen domain component. 1 - Power budget should be applied to given component in domain (volatile setting).
--component_id	<p>If the Per Component Control flag is set, this field contains component identifier for which power budget should be returned. Otherwise, the value in this field is ignored.</p> <ol style="list-style-type: none"> <li>1. For the CPU Domain, the component identifier is the CPU socket number (0–7), where 0 refers to the lowest numbered address on the PECI bus.</li> <li>2. For the Memory Domain, the component identifier is the CPU socket number (0–7), where 0 refers to the lowest numbered address on the PECI bus associated with the memory channels.</li> <li>3. For the PCIe Domain, the component identifier is the PCIe card index.</li> </ol>

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id <Domain ID> --value <assignment value> --per_component_control <Per-component Control> --component_id <Component ID>
In-Band	saa -c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id <Domain ID> --value <assignment value> --per_component_control <Per-component Control> --component_id <Component ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id <Domain ID> --value <assignment value> --per_component_control <Per-component Control> --component_id <Component ID>

Example:

---

## OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id 0 --value 100 --per_component_control 1 --component_id 0
```

## In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id 0 --value 100 --per_component_control 1 --component_id 0
```

## Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id 0 --value 100 --per_component_control 1 --component_id 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.

### 5.17.2.2.8. Deleting Total Power Budget

Use the GeneralNmManage command with the --action DelTotalPower option to delete the total power budget from the managed system.

The following is the supported option for option --action DelTotalPower.

Option	Description
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)

-- per_component_control	Allows for setting the power budget for chosen domain component. 1 - Power budget should be applied to given component in domain (volatile setting).
--component_id	<p>If the Per Component Control flag is set, this field contains component identifier for which power budget should be returned. Otherwise, the value in this field is ignored.</p> <ol style="list-style-type: none"> <li>1. For the CPU Domain, the component identifier is the CPU socket number (0–7), where 0 refers to the lowest numbered address on the PECE bus.</li> <li>2. For the Memory Domain, the component identifier is the CPU socket number (0–7), where 0 refers to the lowest numbered address on the PECE bus associated with the memory channels.</li> <li>3. For the PCIe Domain, the component identifier is the PCIe card index.</li> </ol>

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action DelTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID>
In-Band	saa -c GeneralNmManage --type BMC10 --action DelTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action DelTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action DelTotalPower --domain_id 0 --
per_component_control 1 --component_id 0
```

#### In-Band:



```
[SAA_HOME]# ./saa -c GeneralNmManage --type BMC10 --action DelTotalPower
--domain_id 0 --per_component_control 1 --component_id 0
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action DelTotalPower --domain_id 0 --per_component_control 1
--component_id 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.

#### 5.17.2.2.9. Setting Power Draw Range

Use the GeneralNmManage command with the --action SetPowerDrawRange option to set the BMC Intel Node Manager power draw range from the managed system.

The following options are supported for the --action SetPowerDrawRange option.

Option	Description
--domain_id	0: Entire platform, AC power (Psys support is required) 1: CPU subsystem 2: Memory subsystem 4: PCIe devices subsystem (Psys support is required) 5: Entire platform, DC power (Psys support is required)
--range	Specifies the power draw range. Power draw range: 0-32767

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action SetPowerDrawRange --

	domain_id <Domain ID> --range <Range>
In-Band	saa -c GeneralNmManage --type BMC10 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range>
<b>Multiple Systems</b>	
OoB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range>

Example:

**OoB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action SetPowerDrawRange --domain_id 0 --
range 0-32767
```

**In-Band:**

```
[SAA_HOME]# ./saa -c GeneralNmManage --type BMC10 --action
SetPowerDrawRange --domain_id 0 --range 0-32767
```

**Multiple OoB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action SetPowerDrawRange --domain_id 0 --range 0-32767
```

```
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.

#### 5.17.2.2.10. Getting BMC Intel Node Manager Summary

Use the GeneralNmManage command with the --action GetSummary option to get the summary of BMC Intel Node Manager from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GeneralNmManage --type BMC10 --action GetSummary
In-Band	saa -c GeneralNmManage --type BMC10 --action GetSummary
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action GetSummary

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GeneralNmManage --type BMC10 --action GetSummary
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GeneralNmManage -
-type BMC10 --action GetSummary
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GeneralNmManage --
type BMC10 --action GetSummary
```

```
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.

## 5.17.3 CPU Management

NmCpuManage command can manage CPU configuration by Intel Intelligent Power Node Manager for Supermicro Intel platforms.

The following table summarizes the supported actions in NmCpuManage command with each Intel node manager version.

Option	--type	--action
Description	NM20 = Node manager 2.0	GetPState = Gets the maximum allowed CPU P-State GetTState = Gets the maximum allowed CPU T-State GetPTState = Gets the CPU P-State and T-State GetCPUCores = Gets the maximum allowed logical processors GetCPUMemTemp = Gets the CPU/Memory temperature GetHostCPUData = Gets the host CPU data SetMaxAllowedPState = Sets the maximum allowed CPU P-State SetMaxAllowedTState = Sets the maximum allowed CPU T-State SetMaxAllowedCPUCores = Sets the maximum allowed logical processors
Description	NM40 = Node manager 4.0	GetTurboSyncRatio = Gets the turbo synchronization ratio SetTurboSyncRatio = Sets the turbo synchronization ratio



**Note:**

- Starting from X14 and later platforms, the --type NM20 and NM40 options are not supported. These platforms do not have a Management Engine (ME) to support Intel Node Manager management.

The following chapters will describe each action in detail.

### 5.17.3.1 Intel Intelligent Power Node Manager V2.0

#### 5.17.3.1.1 Getting the Maximum Allowed CPU P-State

Use the NmCpuManage command with option --action GetPState to get the maximum allowed CPU P-state from managed system.

**Single System**

OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action GetPState
In-Band	saa -c NmCpuManage --type NM20 --action GetPState
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetPState

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetPState
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetPState
```

**The console output contains the following information.**

```
Current maximum allowed P-State: 0
Number of P-State: 16
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetPState
```

```
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.

---

### 5.17.3.1.2 Getting the Maximum Allowed CPU T-State

Use the NmCpuManage command with option --action GetTState to get the maximum allowed CPU T-state from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action GetTState
In-Band	saa -c NmCpuManage --type NM20 --action GetTState
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetTState

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetTState
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetTState
```

The console output contains the following information.

```
Current maximum allowed T-State: 0
Number of T-State: 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetTState
```

```
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.

### 5.17.3.1.3 Getting the CPU P-State and T-State

Use the NmCpuManage command with option --action GetPTState to get the CPU P-State and T-State from managed system

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action GetPTState
In-Band	saa -c NmCpuManage --type NM20 --action GetPTState
Multiple Systems	
OOB	saa -I < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetPTState

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetPTState
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetPTState
```

The console output contains the following information.

```
P-State: High |#_____| Low [0/16] (Current/Number of State)
T-State: High |#| Low [0/1] (Current/Number of State)
```

---

## Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetPTState
```

```
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.

### 5.17.3.1.4 Getting the Maximum Allowed Logical Processors

Use the NmCpuManage command with option --action GetCPUCores to get the maximum allowed logical processors from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action GetCPUCores
In-Band	saa -c NmCpuManage --type NM20 --action GetCPUCores
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetCPUCores

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetCPUCores
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetCPUCores
```



---

The console output contains the following information.

```
Current maximum allowed cores: 152
Number of logical cores on the platform: 152
Number of installed processor packages: 2
Number of logical cores on each processor: 76
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type
NM20 --action GetCPUCores
```

```
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.

#### 5.17.3.1.5 Getting the CPU/Memory Temperature

Use the NmCpuManage command with option --action GetCPUMemTemp to get the CPU/Memory temperature from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action GetCPUMemTemp
In-Band	saa -c NmCpuManage --type NM20 --action GetCPUMemTemp
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetCPUMemTemp

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --
type NM20 --action GetCPUMemTemp
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --
type NM20 --action GetCPUMemTemp
```

**The console output contains the following information.**

```
CPU#0 = 38(c) (TJMax = 104, DTS = 66)
CPU#1 = 35(c) (TJMax = 104, DTS = 69)
[CPU#0]CHANNEL#0, DIMM#0 = 39(c)
[CPU#0]CHANNEL#2, DIMM#0 = 38(c)
[CPU#1]CHANNEL#0, DIMM#0 = 39(c)
[CPU#1]CHANNEL#2, DIMM#0 = 37(c)
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type
NM20 --action GetCPUMemTemp
```

```
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.

#### **5.17.3.1.6 Getting the Host CPU Data**

Use the NmCpuManage command with option --action GetHostCPUData to get the host CPU data from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action GetHostCPUData

In-Band	saa -c NmCpuManage --type NM20 --action GetHostCPUDData
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetHostCPUDData

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetHostCPUDData
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetHostCPUDData
```

**The console output contains the following information.**

```
Host CPU data:
End of POST notification was received
Host CPU discovery data is valid
Number of P-States = 16
Number of T-States = 1
Number of installed CPUs/socket = 2
Processor Discovery Data-1 = 00 00 00 00 00 00 00 00
Processor Discovery Data-2 = 00 00 00 00 00 00 00 00
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetHostCPUDData
```

```
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.

#### 5.17.3.1.7 Setting the Maximum Allowed CPU P-State

Use the NmCpuManage command with option --action SetMaxAllowedPState to set the maximum allowed CPU P-State from managed system.

The following are the supported options for option --action SetMaxAllowedPState.

Option	Description
--value	Specifies the maximum allowed CPU P-State. Checks number of P-State by GetPState action.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value <assignment value>
In-Band	saa -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value <assignment value>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value <assignment value>

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value 0
```

##### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value 0
```

The console output contains the following information.

```
NmCpuManage command is completed.
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value 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.

#### 5.17.3.1.8 Setting the Maximum Allowed CPU T-State

Use the NmCpuManage command with option --action SetMaxAllowedTState to set the maximum allowed CPU T-State from managed system.

The following are the supported options for option --action SetMaxAllowedTState.

Option	Description
--value	Specifies the maximum allowed CPU T-State. Checks number of T-State by GetTState action.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value <assignment value>
In-Band	saa -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value <assignment value>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value

	<assignment value>
--	--------------------

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value 0
```

The console output contains the following information.

```
NmCpuManage command is completed.
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value 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.

#### 5.17.3.1.9 Setting the Maximum Allowed Logical Processors

Use the NmCpuManage command with option --action SetMaxAllowedCPUCores to set max allowed logical processors from managed system.

The following are the supported options for option --action SetMaxAllowedCPUCores.

Option	Description
--------	-------------

--value	Specifies the maximum allowed CPU T-State. Checks number of logical cores by GetCpuCores action.
---------	-----------------------------------------------------------------------------------------------------

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value <assignment value>
In-Band	saa -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value <assignment value>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value <assignment value>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value 0
```

The console output contains the following information.

```
NmCpuManage command is completed.
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value 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.

### 5.17.3.2 Intel Intelligent Power Node Manager V4.0

#### 5.17.3.2.1 Getting the Turbo Synchronization Ratio

Use the NmCpuManage command with option --action GetTurboSyncRatio to get the turbo synchronization ratio from managed system.

The following are the supported options for option --action GetTurboSyncRatio.

Option	Description
--socket	CPU socket number. 0~7 - For which current settings should be read. 255 - All sockets will return common maximum settings.
--core	Active cores configuration. 255 - All sockets will return common maximum settings.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM40 --action GetTurboSyncRatio --socket <Socket number> --core <Core number>
In-Band	saa -c NmCpuManage --type NM40 --action GetTurboSyncRatio --socket <Socket number> --core <Core number>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM40 --action GetTurboSyncRatio --socket <Socket number> --core <Core number>



---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --
type NM40 --action GetTurboSyncRatio --socket 0 --core 255
```

**In-Band:**

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --
type NM40 --action GetTurboSyncRatio --socket 0 --core 255
```

**The console output contains the following information.**

```
TurboRatio:
[curTurboRatioLimit=0]
[defTurboRatioLimit=24]
[maxTurboRatioLimit=32]
[minTurboRatioLimit=8]
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type
NM40 --action GetTurboSyncRatio --socket 0 --core 255
```

```
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.

#### 5.17.3.2.2 Setting the Turbo Synchronization Ratio

Use the NmCpuManage command with option --action SetTurboSyncRatio to get the turbo synchronization ratio from managed system.

The following are the supported options for option --action SetTurboSyncRatio.

Option	Description
--socket	CPU socket number. 0~7 - For which current settings should be read. 255 - All sockets will return common maximum settings.
--limit	Turbo Ratio Limit. 0 - Restore default settings. Others - Turbo Ratio Limit to set.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket <Socket number> --limit <limit>
In-Band	saa -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket <Socket number> --limit <limit>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket <Socket number> --limit <limit>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket 0 --limit 0
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket 0 --limit 0
```

The console output contains the following information.

Done

---

## Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket 0 --limit 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.

### 5.17.4 Managing Compute Usage Per Second

NmCupsManage command can manage Compute Usage Per Second (CUPS) by Intel Intelligent Power Node Manager for Supermicro Intel platforms.

The following table summarizes the supported actions in NmCupsManage command with each Intel node manager version.

Option	--type	--action
Description	NM30 = Node manager 3.0	GetCUPSCapability = Get CUPS capability GetCUPSData = Get CUPS data GetCUPSConfig = Get CUPS configuration GetCUPSPolicy = Get CUPS policies GetCUPSCore = Get core CUPS utilization GetCUPSIO = Get IO CUPS utilization GetCUPSMem = Get memory CUPS utilization SetCUPSPolicy = Set CUPS policy EnableCUPSPolicy = Enable CUPS policy DisableCUPSPolicy = Disable CUPS Policy



#### Notes:

- Starting from X14 and later platforms, the --type NM30 option is not supported. These platforms do not have a Management Engine (ME) to support Intel Node Manager management.

---

### 5.17.4.1 Getting the CPUS Capability

Use the NmCupsManage command with option --action GetCUPSCapability to get the compute usage per second (CUPS) capability from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action GetCUPSCapability
In-Band	saa -c NmCupsManage --type NM30 --action GetCUPSCapability
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSCapability

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSCapability
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSCapability
```

**The console output contains the following information.**

```
CUPS Capabilities: CUPS feature is enabled
CUPS Policy : CUPS policies configuration available
CUPS version : 1
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action GetCUPSCapability
```

```
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.

#### 5.17.4.2 Getting the CUPS Data

Use the NmCupsManage command with option --action GetCUPSDData to get the compute usage per second (CUPS) data from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action GetCUPSDData
In-Band	saa -c NmCupsManage --type NM30 --action GetCUPSDData
Multiple Systems	
OOB	saa -I < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSDData

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSDData
```

##### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSDData
```

**The console output contains the following information.**

```
CUPS Index: 0
CUPS Dynamic Load Factors:
 CPU CUPS dynamic Load factor : 0
 Memory CUPS dynamic Load factor : 0
 IO CUPS dynamic Load factor : 0
```

```

Base Utilization:
 Base CPU CUPS utilization value : 00 00 FF FF FF FF FF FF

Aggregate utilization values:
 Aggregate CPU CUPS utilization value : 4D 8C 9C 05 00 00 00 00
 Aggregate Memory CUPS utilization value : 0F 76 02 00 00 00 00 00
 Aggregate IO CUPS utilization value : 50 48 00 00 00 00 00 00

Utilization Average:
 Utilization average for the core domain : 0% (00 00 00 00 00 00 00 00)
 Utilization average for the memory domain : 0% (00 00 00 00 00 00 00 00)
 Utilization average for the IO domain : 0% (00 00 00 00 00 00 00 00)

```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action GetCUPSData
```

```

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.

#### 5.17.4.3 Getting the CUPS Configuration

Use the NmCupsManage command with option --action GetCUPSConfig to get the compute usage per second (CUPS) configuration from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action GetCUPSConfig
In-Band	saa -c NmCupsManage --type NM30 --action GetCUPSConfig
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSConfig

---

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSConfig
```

**In-Band:**

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSConfig
```

**The console output contains the following information.**

```
CUPS Feature Enabled Status : CUPS feature is enabled
Load Factor Configuration : Dynamic
Static Core Load Factor : 1
Static Memory Load Factor : 1
Static IO Load Factor : 1
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action GetCUPSConfig
```

```
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.

#### 5.17.4.4 Getting the CUPS Policies

Use the NmCupsManage command with option --action GetCUPSPolicy to get the compute usage per second (CUPS) policies from managed system.

<b>Single System</b>
----------------------

OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action GetCUPSPolicy
In-Band	saa -c NmCupsManage --type NM30 --action GetCUPSPolicy
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSPolicy

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSPolicy
```

**In-Band:**

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSPolicy
```

**The console output contains the following information.**

```
CUPS Policy ID : Core Domain
Target identifier : BMC
Policy Status : Policy Enabled
Policy Storage : Persistent storage
Policy Excursion Actions : Sending of alert enabled
CUPS Threshold : 0
Averaging Window in sec : 6
```

```
CUPS Policy ID : Memory Domain
Target identifier : BMC
Policy Status : Policy Enabled
Policy Storage : Persistent storage
Policy Excursion Actions : Sending of alert enabled
CUPS Threshold : 0
Averaging Window in sec : 6
```

```
CUPS Policy ID : IO Domain
Target identifier : BMC
Policy Status : Policy Enabled
Policy Storage : Persistent storage
Policy Excursion Actions : Sending of alert enabled
CUPS Threshold : 0
```



---

```
Averaging Window in sec : 6
```

```
CUPS Policy ID : Core Domain
Target identifier : Remote Console
Policy Status : Policy Enabled
Policy Storage : Persistent storage
Policy Excursion Actions : Sending of alert enabled
CUPS Threshold : 0
Averaging Window in sec : 6
```

```
CUPS Policy ID : Memory Domain
Target identifier : Remote Console
Policy Status : Policy Enabled
Policy Storage : Persistent storage
Policy Excursion Actions : Sending of alert enabled
CUPS Threshold : 0
Averaging Window in sec : 6
```

```
CUPS Policy ID : IO Domain
Target identifier : Remote Console
Policy Status : Policy Enabled
Policy Storage : Persistent storage
Policy Excursion Actions : Sending of alert enabled
CUPS Threshold : 0
Averaging Window in sec : 6
```

### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action GetCUPSPolicy
```

```
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.

#### 5.17.4.5 Getting the Core CUPS Utilization

Use the NmCupsManage command with option --action GetCUPSCore to get the core compute usage per second (CUPS) utilization from managed system.

<b>Single System</b>
----------------------

OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action GetCUPSCore
In-Band	saa -c NmCupsManage --type NM30 --action GetCUPSCore
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSCore

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSCore
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSCore
```

The console output contains the following information.

```
Core CUPS = 0
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action GetCUPSCore
```

```
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.

### 5.17.4.6 Getting the IO CUPS Utilization

---

Use the NmCupsManage command with option --action GetCUPSIO to get the IO compute usage per second (CUPS) utilization from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action GetCUPSIO
In-Band	saa -c NmCupsManage --type NM30 --action GetCUPSIO
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSIO

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSIO
```

**In-Band:**

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSIO
```

**The console output contains the following information.**

```
IO CUPS = 0
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action GetCUPSIO
```

```
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.

#### 5.17.4.7 Getting the Memory CUPS Utilization

Use the NmCupsManage command with option --action GetCUPSMem to get the memory compute usage per second (CUPS) utilization from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action GetCUPSMem
In-Band	saa -c NmCupsManage --type NM30 --action GetCUPSMem
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSMem

Example:

##### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSMem
```

##### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action GetCUPSMem
```

**The console output contains the following information.**

```
Memory CUPS = 0
```

##### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action GetCUPSMem
```

```
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.

#### 5.17.4.8 Setting CUPS Policy

Use the NmCupsManage command with option --action SetCUPSPolicy to set the compute usage per second (CUPS) policy from managed system.

The following are the supported options for option --action SetCUPSPolicy.

Option	Description
--domain_id	Domain ID 1: Core Domain 2: Memory Domain 4: IO Domain
--storage	Storage 0: Persistent storage 1: Volatile memory
--alert	Alert 0: Disable alerting 1: Enable sending of alert
--threshold	Threshold Assigns CUPS threshold (0-100).
--avg_window	averaging window Assigns averaging window in seconds (0-65535).

#### Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action SetCUPSPolicy --domain_id <Domain ID> --storage <Storage> --alert <Alert> --threshold <Threshold> --avg_window <averaging window>
In-Band	saa -c NmCupsManage --type NM30 --action SetCUPSPolicy --domain_id <Domain ID> --storage <Storage> --alert <Alert> --threshold <Threshold> --avg_window <averaging window>
<b>Multiple Systems</b>	
OOB	saa -I < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action SetCUPSPolicy --domain_id <Domain ID> --storage <Storage> --alert <Alert> --threshold <Threshold> --avg_window <averaging window>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action SetCUPSPolicy --domain_id 1 --storage 1 --alert 1 -
threshold 50 --avg_window 2000
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action SetCUPSPolicy --domain_id 1 --storage 1 --alert 1 -
threshold 50 --avg_window 2000
```

**The console output contains the following information.**

```
Done.
CUPS Policy ID : Core Domain
Target identifier : Remote Console
Policy Status : Policy Enabled
Policy Storage : Volatile memory
Policy Excursion Actions : Sending of alert enabled
CUPS Threshold : 50
Averaging Window in sec : 2000
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action SetCUPSPolicy --domain_id 1 --storage 1 --alert 1 --
threshold 50 --avg_window 2000
```

```
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.

#### 5.17.4.9 Enabling the CUPS Policy

Use the NmCupsManage command with option --action --EnableCUPSPolicy to enable the compute usage per second (CUPS) policy from managed system.

The following are the supported options for option --action EnableCUPSPolicy.

Option	Description
--domain_id	Domain ID 1: Core Domain 2: Memory Domain 4: IO Domain

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action EnableCUPSPolicy --domain_id <Domain ID>
In-Band	saa -c NmCupsManage --type NM30 --action EnableCUPSPolicy --domain_id <Domain ID>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action EnableCUPSPolicy --domain_id <Domain ID>

Example:

---

## OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action EnableCUPSPolicy --domain_id 1
```

## In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action EnableCUPSPolicy --domain_id 1
```

The console output contains the following information.

```
Done.
```

## Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action EnableCUPSPolicy --domain_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.

### 5.17.4.10 Disabling the CUPS Policy

Use the NmCupsManage command with option --action --DisableCUPSPolicy to enable the compute usage per second (CUPS) policy from managed system.

The following are the supported options for option --action DisableCUPSPolicy.

Option	Description
--domain_id	Domain ID 1: Core Domain



	2: Memory Domain 4: IO Domain
--	----------------------------------

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NmCupsManage --type NM30 --action DisableCUPSPolicy --domain_id <Domain ID>
In-Band	saa -c NmCupsManage --type NM30 --action DisableCUPSPolicy --domain_id <Domain ID>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action DisableCUPSPolicy --domain_id <Domain ID>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action DisableCUPSPolicy --domain_id 1
```

#### In-Band:

```
[SAA_HOME]# ./saa -c -I Redfish_HI -u ADMIN -p PASSWORD -c NmCupsManage -
-type NM30 --action DisableCUPSPolicy --domain_id 1
```

**The console output contains the following information.**

```
Done.
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCupsManage --
type NM30 --action DisableCUPSPolicy --domain_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.

### 5.17.5. Managing BMC Intel Node Manager

The BmcNmManage command can manage BMC Intel node manager through Intel Intelligent Power Node Manager for Supermicro Intel platforms.

The following table summarizes the supported actions in BmcNmManage command for each Intel Node Manager version.

Option	--type	--action
Description	BMC10 = BMC Intel Node Manage 1.0	GetDeviceID = Gets BMC device ID GetPower = Gets power information from BMC GetTemp = Gets temperature information from BMC

Each action is described in detail in the following sections.

#### 5.17.5.1. Getting a BMC Device ID

Use the BmcNmManage command with the --action GetDeviceID option to get the BMC device ID from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BmcNmManage --type BMC10 --action GetDeviceID
In-Band	saa -c BmcNmManage --type BMC10 --action GetDeviceID
Multiple Systems	

---

OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c BmcNmManage --type BMC10 --action GetDeviceID</code>
-----	-----------------------------------------------------------------------------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BmcNmManage --type BMC10 --action GetDeviceID
```

**In-Band:**

```
[SAA_HOME]# ./saa -c BmcNmManage --type BMC10 --action GetDeviceID
```

**The console output contains the following information.**

```
Device ID = 20h
Firmware Version = 0.0.2
IPMI Version = 2.0
Manufacturer ID = 7C 2A 00
Board ID = 27 1D
Raw Data = 20 01 00 02 02 BF 7C 2A 00 27 1D 02 02 00 00
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BmcNmManage --type BMC10 --action GetDeviceID
```

```
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.

### 5.17.5.2. Getting Power Information from BMC

---

Use the BmcNmManage command with the --action GetPower option to get power information of managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BmcNmManage --type BMC10 --action GetPower
In-Band	saa -c BmcNmManage --type BMC10 --action GetPower
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcNmManage --type BMC10 --action GetPower

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BmcNmManage --type BMC10 --action GetPower
```

**In-Band:**

```
[SAA_HOME]# ./saa -c BmcNmManage --type BMC10 --action GetPower
```

**The console output contains the following information.**

```
56 watts
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BmcNmManage --type BMC10 --action GetPower
```

```
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.

### 5.17.5.3. Getting Temperature Information from BMC

Use the BmcNmManage command with the --action GetTemp option to get the temperature information of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BmcNmManage --type BMC10 --action GetTemp
In-Band	saa -c BmcNmManage --type BMC10 --action GetTemp
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcNmManage --type BMC10 --action GetTemp

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BmcNmManage --type BMC10 --action GetTemp
```

#### In-Band:

```
[SAA_HOME]# ./saa -c BmcNmManage --type BMC10 --action GetTemp
```

The console output contains the following information.

```
56 (C)
```

#### Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BmcNmManage --type BMC10 --action GetTemp
```

```
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.

## 5.18. Security Management

### 5.18.1. TPM Management

The “TpmProvision” command can be executed to enable TPM module capabilities and clear TPM module capabilities for the managed system.

Through OTA TPM technologies, the “GetTpmInfo” and “TpmManage” commands can be executed to receive TPM information and manage TPM, respectively. SAA 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 ( <b>Legacy</b> )	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
-----------------------	-----	-----	----------



**Note:**

TpmManage command is not supported on AMD platforms.

### 5.18.1.1. Getting TPM Information

Use the “GetTpmInfo” command to get the TPM module information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetTpmInfo [--showall]
In-Band	saa -c GetTpmInfo [--showall]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetTpmInfo [--showall]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetTpmInfo --showall
```

**In-Band:**

```
[SAA_HOME]# ./saa -c GetTpmInfo --showall
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -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.

**The console output contains the following information when installing the TPM 1.2 module.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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: 0x500000001
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
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 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
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
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

```

## 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 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.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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 GetTpmlInfo 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 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
```

#### 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 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

```



### 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 only be displayed when the option --showall is assigned.

- This command will query the TPM module information through Intel OTA or Supermicro OTA.

#### 5.18.1.2. Provisioning the TPM Module

On X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets and later platforms, use the “TpmManage” command to execute SAA to enable the TPM module capabilities for the managed system. Before executing the command, the TPM module should be installed on the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c TpmManage --provision [options...]
In-Band	saa -c TpmManage --provision [options...]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c TpmManage [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:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --provision --table_default --reboot
```



---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --provision --table Tpm12Prov.bin --reboot
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c TpmManage --provision --table_default --reboot
```

```
[SAA_HOME]# ./saa -c TpmManage --provision --table Tpm12Prov.bin --reboot
```

#### **Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TpmManage --provision --table_default --reboot
```

```
[SAA_HOME]# ./saa -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.



#### **Notes:**

- This command is supported on X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets or later platforms.
- The system may reboot several times during provisioning.
- Please execute the GetTpmInfo command to obtain OTA supported type before doing TPM provision.
- The TPM module will be 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.

- When using TPM provision 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 SAA to enable TPM module capabilities for the managed system. Before executing the command, the TPM module should be installed on the managed system.

Single System	
OOB	saa -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>]]
Multiple Systems	
OOB	saa -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:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmProvision -
-image_url 'smb://192.168.35.1/MySharedPoint/MyFolder' --id smbaid --pw
smbpasswd --reboot --lock yes
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmProvision -
-image_url 'http://192.168.35.1/MySharedPoint/MyFolder' --id smbaid --pw
```

---

```
smbpasswd --reboot --lock yes
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmProvision -
-image_url '\192.168.35.1\MySharedPoint\MyFolder' --id smbuid --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 SAA package. This ISO image can be acquired from Supermicro. Each SAA release could require different ISO images as noted in SAA release notes. Please acquire the correct TPM\_version\_YYYYMMDD.zip, unzip the zip file and get the TPM ISO images for usage.
- With TPM ISO images, TPM capabilities can be enabled or cleared.
- The BIOS will reboot several times during provisioning.
- To clear TPM capability, see 5.18.1.3 Enabling and Clearing the TPM Module Capabilities.
- Space is prohibited for a SAMBA password. SAA 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, exit code 37 will be returned.
- The --cleartpm option clears the ownership of the TPM module.
- The --lock yes option locks the TPM module.
- SAA will stop TPM provision procedures if the CPU or platform does not support Intel Trusted Execution Technology (Intel TXT).

---

#### 5.18.1.3. Enabling and Clearing the 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 for 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c TpmManage {options...} [--reboot]
In-Band	saa -c TpmManage {options...} [--reboot]
Multiple Systems	
Multiple Systems	saa -l <system list file> [-u <username> -p <password>] -c TpmManage {options...} [--reboot]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --clear_and_enable_dtpm_txt --reboot
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --clear_dtpm --reboot
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --enable_txt_and_dtpm --reboot
```

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --clear_and_enable_dtpm --reboot
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --disable_dtpm --reboot
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmManage --disable_txt --reboot
```

#### **In-Band :**

```
[SAA_HOME]# ./saa -c TpmManage --clear_and_enable_dtpm_txt --reboot
```

```
[SAA_HOME]# ./saa -c TpmManage --clear_dtpm --reboot
```

```
[SAA_HOME]# ./saa -c TpmManage --enable_txt_and_dtpm --reboot
```

```
[SAA_HOME]# ./saa -c TpmManage --clear_and_enable_dtpm --reboot
```

```
[SAA_HOME]# ./saa -c TpmManage --disable_dtpm --reboot
```

```
[SAA_HOME]# ./saa -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 SAA will remind the user to reboot manually.
- The options of each use case are mutually exclusive.
- The “--disable\_dtpm” option is not supported from 14th generation Intel platform.

---

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 [5.18.1.2. Provisioning the TPM Module](#)

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c TpmProvision --image_url <URL> [--id <id for URL> --pw <password for URL>] --cleartpm --reboot
Multiple Systems	
Multiple Systems	saa -l <system list file> [-u <username> -p <password>] -c TpmProvision --image_url <URL> [--id <id for URL> --pw <password for URL>] --cleartpm --reboot

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c TpmProvision -
-image_url 'smb://192.168.35.1/MySharedPoint/MyFolder' --id smbids --pw
smbpasswd --cleartpm --reboot
```

**Multiple OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TpmProvision --
image_url 'smb://192.168.35.1/MySharedPoint/MyFolder' --id smbids --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.

---

## 5.18.2. Managing BIOS RoT Functions

The “BiosRotManage” command supports the following features on RoT systems:

---

- **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 [5.8.3 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 restricted 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.

---

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BiosRotManage --action <action> [--redfish] [--file <evidence.bin.gz> [-overwrite]] [--reboot]

In-Band	saa -I Redfish_HI -u <username> -p <password> -c BiosRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]] [--reboot]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> [--remote_saa <remote SAA path>] -c BiosRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]] [--reboot]
<b>Multiple Systems</b>	
OOB	saa -I <system list file> [-u <username> -p <password>] -c BiosRotManage --action <action> [--redfish] [--file <evidence.bin.gz> [--overwrite]] [--reboot]
Remote In-Band	saa -I Remote_RHI -I <system list file> [--remote_saa <remote SAA path>] -c BiosRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]] [--reboot]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -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
the system 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.
.....
.....
.....
.....
```

```
[SAA_HOME]# ./saa -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:**

```
[SAA_HOME]# ./saa -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.....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
```

### **Remote In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --ou 192.168.34.56 -
--ou root --op 111111 --BiosRotManage --action GetInfo --remote_saa
/root/saa
```

### **The console output contains the following information.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.56:
=====
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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/saa.log' from
'/root/saa_remote_inband/2022-11-09_13-37-05/saa.log' on 192.168.34.56.

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

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -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
```

### 5.18.3. Managing BMC RoT Functions

The “BmcRotManage” command supports the following features on RoT systems:

- **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 [5.8.3 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 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.

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c BmcRotManage --action &lt;action&gt; [--file &lt;evidence.bin.gz&gt; [--overwrite]]</code>
In-Band	<code>saa -l Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c BmcRotManage --action &lt;action&gt; [--file &lt;evidence.bin.gz&gt; [--overwrite]]</code>
Remote In-Band	<code>saa -l Remote_RHI -u &lt;username&gt; -p &lt;password&gt; --oi &lt;OS IP address&gt; --ou &lt;OS username&gt; --op &lt;OS password&gt; [--remote_saa &lt;remote SAA path&gt;] -c BmcRotManage --action &lt;action&gt; [--file &lt;evidence.bin.gz&gt; [--overwrite]]</code>
Multiple Systems	
OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c BmcRotManage --action &lt;action&gt; [--file &lt;evidence.bin.gz&gt; [--overwrite]]</code>
Remote In-Band	<code>saa -l Remote_RHI -l &lt;system list file&gt; [--remote_saa &lt;remote SAA path&gt;] -c BmcRotManage --action &lt;action&gt; [--file &lt;evidence.bin.gz&gt; [--overwrite]]</code>

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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 through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -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:**

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

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -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
```

### 5.18.4. Managing CPLD RoT Functions

The “CpldRotManage” command supports the following features on RoT systems of X13 RoT2.0 and later platforms:

- **Getting Information on CPLD**  
Use the “CpldRotManage” command with the option “--action GetInfo” to retrieve information on active CPLD and golden CPLD.
- **Updating the Golden Image**  
Use the “CpldRotManage” command with the “--action UpdateGolden” option to replace the golden image with an active CPLD firmware.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CpldRotManage --action <action>
In-Band	saa -I Redfish_HI -u <username> -p <password> -c CpldRotManage --action <action>

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c CpldRotManage --action <action>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CpldRotManage
--action GetInfo
```

The console output contains the following information.

```
Managed system.....192.168.34.56
 CPLD version.....F5.07.02
 Golden CPLD version.....F5.07.01
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CpldRotManage
--action UpdateGolden
```

The console output contains the following information.

```
.....
Status: System is backing up current FW as golden image. Please wait for 2
minutes.
.....
.....
Done
Status: Please check golden FW version for result.
```

#### In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c CpldRotManage --
action UpdateGolden
```

The console output contains the following information.

```
.....
Status: System is backing up current FW as golden image. Please wait for 2
minutes.
```

```
.....
.....
Done
Status: Please check golden FW version for result.
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c CpldRotManage --
action UpdateGolden
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## 5.18.5. 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, SAA will use the current OS time of the managed 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, SAA will use the current OS time of the managed system as the default nonce.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c Attestation --action <action> [--file <filename> [--overwrite] [--item <item name>]] [--ref <filename>] [--nonce <nonce>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c Attestation --action <action> [--file <filename> [--overwrite] [--item <item name>] [--showall] [--file_only]] [--ref <filename>] [--nonce <nonce>]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> [--remote_saa <remote SAA path>] -c Attestation --action <action> [--file <filename> [--overwrite] [--item <item name>]] [--ref <filename>] [--nonce <nonce>]
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c Attestation --action <action> [--file <filename> [--overwrite]]
Remote In-Band	saa -I Remote_RHI -I <system list file> [--remote_saa <remote SAA path>] -c Attestation --action <action> [--file <filename> [--overwrite]]



**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:**

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

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c Attestation --
action Dump
```

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

#### **In-Band through Redfish Host Interface:**

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

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c Attestation --
action Delete --file measurement.bin
```

#### **In-Band:**

```
[SAA_HOME]# ./saa -c Attestation --action GetInfo --file_only --file
measurement.bin
```

#### **Remote In-Band:**

```
[SAA_HOME]# ./saa -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:**

```
[SAA_HOME]# ./saa -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
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -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
```

```
[SAA_HOME]# ./saa -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.
```

```
[SAA_HOME]# ./saa -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:
A30CFFFC59284658300654B8CDD5144B7C8CCDF3540B52EAF98FE0B7A3A8A4BB1E7FEA2D89FC9F7BB7
01B35C1DD53B43E08751F483573DB75E9F3D5653B0871A
```

```
[SAA_HOME]# ./saa -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>
```

---

```
[SAA_HOME]# ./saa -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	Descriptions
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	Descriptions
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	Descriptions
Matched	The Root CA Certificate matches with the input certificate file.
Mismatched	The Root CA Certificate does not match with the input certificate file.

### 5.18.6. Acquiring the BMC System Lockdown Mode

When the System Lockdown Mode is enabled on a managed system, neither setting configurations nor updating firmware is allowed in this mode. To learn about the managed system status, use the “GetLockdownMode” command.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetLockdownMode
In-Band	saa -c GetLockdownMode
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetLockdownMode [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetLockdownMode
Remote In-Band	saa -l Remote_INB -l <system list file> -c GetLockdownMode [--remote_saa <remote SAA path>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -c GetLockdownMode
```

#### Remote In-Band:

```
[SAA_HOME]# ./saa -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
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetLockdownMode
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -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
```

## 5.18.7. Setting the BMC System in Lockdown Mode

Use the “SetLockdownMode” command to have SAA set the BMC system to Lockdown Mode.

Single System	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SetLockdownMode {--lock &lt;yes   no&gt; --reboot}</code>
Multiple Systems	
OOB	<code>saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SetLockdownMode {--lock &lt;yes   no&gt; --reboot}</code>

Example:

#### OOB:

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

---

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetLockdownMode --lock <yes | no> --reboot
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

### 5.18.8. 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.

- **Resetting 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 system secure boot keys through BMC Redfish API.

- **Deleting PK**

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



**Notes:**

- This command is only available on X13/H13 and later platforms.
  - The SFT-DCMS-SINGLE license is required.
  - 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).
  - “dbx” can be only used with the “ShowDatabases” action.
  - The “--file” option” only supports PEM files.
- 

Type	Description
PK	Platform Keys
KEK	Key Exchange Keys
db	Authorized Signatures
dbr	OS Recovery Signatures
dbt	Authorized Timestamps
dbx	Forbidden Signatures

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SecureBootManage --redfish --action <action> [--file_type <file type> [-



	-file <CertificateFile>]] [--reboot [--post_complete]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c SecureBootManage --redfish --action <action> [--file_type <file type> [- -file <CertificateFile>]] [--reboot]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c SecureBootManage --redfish --action <action> [--file_type <file type> [- -file <CertificateFile>]] [--reboot] [--remote_saa <remote SAA path>]
<b>Multiple Systems</b>	
OOB	saa -I <system list file> [-u <username> -p <password>] -c SecureBootManag --redfish --action <action> [--file_type <file type> [-- file <CertificateFile>]] [--individually]] [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_RHI -I <system list file> -c SecureBootManage --redfish --action <action> [--file_type <file type> [--file <CertificateFile>]] [-- individually] [--reboot]

Example:

#### OOB:

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

The console output contains the following information:

```
....
Status: Secure boot is enabled for 192.168.34.56
Note: You have to reboot or power up the system for the BIOS changes to take
effect.
```

```
[SAA_HOME]# ./saa -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 is uploaded for 192.168.34.56
Note: You have to reboot or power up the system for the BIOS changes to take
```

---

effect.

### **In-band:**

```
[SAA_HOME]# ./saa -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:**

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 --ou root --op 111111 -c SecureBootManage --redfish --action Status --remote_saa /root/saa
```

### **The console output contains the following information:**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.

Start Remote In-Band execution on 192.168.34.56:
=====
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 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/saa.log' from
'/root/saa_remote_inband/2023-04-12_13-37-05/saa.log' on 192.168.34.56.

End Remote In-Band execution on 192.168.34.56.

```

## Multiple Systems OOB:

```
[SAA_HOME]# ./saa -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:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SecureBootManage --
redfish --action UploadCertificate --file_type PK --file
CertificateFile.pem -- individually --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
```

### 5.18.9. Securely Erasing Hard Disks Attached to a RAID Controller

Use the “SecureEraseRaidHdd” command to execute SAA to securely erase hard disks (HDD or SSD) in the target RAID controller system and poll the erasing status asynchronously or synchronously.

Single System	
OOB	<ol style="list-style-type: none"><li>1. <code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SecureEraseRaidHdd [--dev_id &lt;device_id&gt; [--enc_id &lt;enclosure id&gt;] [--dsk_id &lt;disk id&gt;] [--sync] [--type &lt;BRCM_IT BRCM_IR&gt;]]   --precheck</code></li><li>2. <code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SecureEraseRaidHdd --tsk_id &lt;task id&gt; [--sync]</code></li></ol>
In-Band	<ol style="list-style-type: none"><li>1. <code>saa -I Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c SecureEraseRaidHdd [--dev_id &lt;device_id&gt; [--enc_id &lt;enclosure id&gt;] [--dsk_id &lt;disk id&gt;] [--sync] [--type &lt;BRCM_IT BRCM_IR&gt;]]   --precheck</code></li></ol>

	2. <code>saa -l Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c SecureEraseRaidHdd --tsk_id &lt;task id&gt; [--sync]</code>
<b>Multiple Systems</b>	
OOB	1. <code>saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SecureEraseRaidHdd [--dev_id &lt;device_id&gt; [--enc_id &lt;enclosure id&gt;] [--dsk_id &lt;disk id&gt;] [--sync] [--type &lt;BRCM_IT BRCM_IR&gt;]]   --precheck</code> 2. <code>saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SecureEraseRaidHdd --tsk_id &lt;task id&gt; [--sync]</code>

To securely erase HDDs in the RAID controller system, follow these steps.

1. Execute the “GetRaidCfg” command to confirm the JBOD mode of the RAID controller system is in “Disabled” state, and the disks to be erased in the 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 RAID controller system. Also, you can use --precheck option to see the model, manufacturer and ID of RAID card, enclosure ID, disk ID, and the F/W state and Secure-Erase support on each disk.

<b>Single System</b>	
OOB	<code>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SecureEraseRaidHdd --precheck</code>
In-Band	<code>saa -l Redfish_HI -u &lt;username&gt; -p &lt;password&gt; -c SecureEraseRaidHdd --precheck</code>
<b>Multiple Systems</b>	
OOB	<code>saa -l &lt; system list file &gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SecureEraseRaidHdd --precheck</code>

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SecureEraseRaidHdd --precheck
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
 Dev_ID Enc_ID Dsk_ID Manufacturer Model FW Status
Support Erase Status

0 0 0 Broadcom SAS 3808 Unconfigured good drive
Yes
0 0 1 Broadcom SAS 3808 Unconfigured good drive
Yes
0 0 2 Broadcom SAS 3808 Unconfigured good drive
Yes
```

### Multiple Systems:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseRaidHdd
--precheck
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

If the execution “Status” field for a managed system shows SUCCESS, the overall list of disk(s) in the RAID Controller systems will be shown in the “Execution Message” section of the managed system in the created log file.

2. Follow the rule below to erase your target physical disk(s) listed in the RAID controller system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SecureEraseRaidHdd --dev_id <device_id> [--enc_id <enclosure id>] [--dsk_id <disk id>] [--sync] [--type <BRCM_IT BRCM_IR>]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c SecureEraseRaidHdd --dev_id <device_id> [--enc_id <enclosure id>] [--dsk_id <disk id>] [--sync] [--type <BRCM_IT BRCM_IR>]

Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SecureEraseRaidHdd --dev_id <device_id> [--enc_id <enclosure id>] [--dsk_id <disk id>] [--sync] [--type <BRCM_IT BRCM_IR>]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)

Copyright(C) 2023 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] : 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.
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseRaidHdd
--dev_id 0 --enc_id 0,1,2 --dsk_id 0,3,4
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseRaidHdd
--dev_id 0 --enc_id ALL --dsk_id ALL --sync
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseRaidHdd
--dev_id 0 --enc_id ALL --dsk_id 0,1,2 --abort
```

```
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 or aborting result of the managed system will be shown in the "Execution Message" section of the managed system in the created log file.

SAA 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/FW 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	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	Enabled	YES	YES	F/W State is not "Unconfigured good drive" (Ex.: Unconfigured Bad Drive./Drive is exposed and controlled by a host./ The configured drive is online...etc)

The following table lists Secure-Erase supported RAID Card by SAA:

Model	Controller
AOC-S3108L-H8iR(-16DD)	Broadcom SAS 3108
AOC-SLG3-2H8M2	Broadcom SAS 3408
AOC-S3808L-L8iR	Broadcom SAS 3808
AOC-S3816L-L16iR	Broadcom SAS 3816
AOC-S3908L-H8iR(-16DD/-32DD)	Broadcom SAS 3908
AOC-S3916L-H16iR(-32DD)	Broadcom SAS 3916



---

AOC-S3808L-L8iT1 <sup>1</sup>	Broadcom SAS 3808
AOC-S3816L-L16iT1 <sup>1</sup>	Broadcom SAS 3816
AOC-SLG4-2H8M2 <sup>1</sup>	Broadcom SAS 4116
AOC-SLG3-2H8M2 <sup>1</sup>	Broadcom SAS 3408

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 further polling status purpose.

You can also poll the erasing status right after issuing the command by appending --sync option after the command "SecureEraseRaidHdd".

Example:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SecureEraseRaidHdd --dev_id 0 --enc_id ALL --dsk_id 0,1,2,3 --sync
```



#### Notes:

- The Secure-Erase function for IT/HBA RAID controller is supported by OEM FW only.
  - 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.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
```

```
Copyright(C) 2023 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 F/W 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	12:53:43	
2	0	0	1	73%	Running	12:54:17	
3	0	0	2	4%	Running	14:32:47	
4	0	0	3	4%	Running	14:32:55	
5	0	1	0	4%	Running	14:33:17	

```
6 | 0 | 1 | 1 | 4% | Running | 14:33:25 |
Polling progress...
```

- Execute the “SecureEraseRaidHdd” command with the --tsk\_id option below to check the erasing status of target disk(s) in the RAID system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SecureEraseRaidHdd --tsk_id <task id> [--sync]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c SecureEraseRaidHdd --tsk_id <task id> [--sync]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SecureEraseRaidHdd --tsk_id <task id> [--sync]



**Note:**

In multiple systems, the --sync option is not allowed with --tsk as polling the erasing status on the RAID controller system.

Example:

**OOB:**

```
[SAA_HOME]# ./saa -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.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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 | 12:53:43 | |
2 | 0 | 0 | 1 | 75% | Running | 12:54:17 | |
3 | 0 | 0 | 2 | 8% | Running | 14:32:47 | |
```

4	0	0	3	8%	Running	14:32:55	
5	0	1	0	7%	Running	14:33:17	
6	0	1	1	7%	Running	14:33:25	

Polling progress...

If the task status becomes “Completed,” the start and elapsed time of task will appear on the console output.

Example:

**00B:**

```
[SAA_HOME]# ./saa -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.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 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.
```

**Multiple Systems 00B:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseRaidHdd
--tsk_id 1,2,3
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

If the execution “Status” field for a managed system shows SUCCESS, the erasing status of the RAID Controller systems will be shown in the “Execution Message” section

---

of the managed system in the created log file.

To abort secure erase HDDs action of the target disk(s) in the RAID controller system, follow these two steps as below.

1. Execute the "SecureEraseRaidHdd" command to erase the target disk(s) in the RAID system.
2. Execute the "SecureEraseRaidHdd" command with --abort option below to stop the currently erasing target disk(s) in the RAID system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SecureEraseRaidHdd --dev_id <device_id> [--enc_id <enclosure id>] [--dsk_id <disk id>] [--abort]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c SecureEraseRaidHdd --dev_id <device_id> [--enc_id <enclosure id>] [--dsk_id <disk id>] [--abort]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SecureEraseRaidHdd --dev_id <device_id> [--enc_id <enclosure id>] [--dsk_id <disk id>] [--abort]

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SecureEraseRaidHdd --dev_id 0 --enc_id 0 --dsk_id 2,3 --abort
```

**The console output contains the following information.**

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)

Copyright(C) 2023 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 F/W state of each disk...

The F/W STATE of EACH DISK :

[--dev\_id:--enc\_id:--dsk\_id] : F/W State

[ 0: 0: 2] : Unconfigured good drive

[ 0: 0: 3] : Unconfigured good drive

Start aborting securely erasing each disk...

.....Finish aborting Secure-Erase progress.

Example:

**00B:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SecureEraseRaidHdd --dev_id 0 --enc_id 0 --dsk_id 0,1 --abort
```

**The console output contains the following information.**

SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86\_64)

Copyright(C) 2023 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 F/W 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

Start aborting securely erasing each disk...

*****<<<<ERROR>>>>*****

ExitCode = 120

Description = Invalid Redfish response

Program Error Code = 440.24

Error message:

 The following disk list fail to abort for Secure Erase action.

 The list format is [--dev_id:--enc_id:--dsk_id]

 1. [0:0:1]

```

### Multiple Systems 00B:

```

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseRaidHdd
--dev_id 0 --enc_id ALL --dsk_id 0,1,2 --abort

```

```

SList.txt:
192.168.34.56
192.168.34.57

```

If the execution “Status” field for a managed system shows SUCCESS, the erasing status of the RAID Controller systems will be shown in the “Execution Message” section of the managed system in the created log file.

SAA will check the list of target disk(s) for aborting process and display the success prompt when all the target disks can be successfully aborted. When the target disk(s) cannot execute abort action, SAA will show the list of the target disk(s) to notify user.

**Note:**

The SecureEraseRaidHdd command is supported on X12/H12 and later platforms.

### 5.18.10. Securely Erasing Hard Disks

Use the “SecureEraseDisk” command to have SAA 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, SAA 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 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, 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, the 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.

SAA maps the PSID and password to the target HDD on the managed system automatically based on serial numbers. The following is an example of PSID.txt and Password.txt:

Assume there is a system installed with one SAT3 supported device and one TCG supported device:

Security Mode	Serial Number	PSID	Password	New Password
---------------	---------------	------	----------	--------------

SAT3	9XF4AF7M	N/A	123456	111111
TCG	W472TJXH	HR1MJDCK LH4CD88EL EGDUE5J4 UA3QGZZ	123456	111111

#### PSID.txt

```
W472TJXH; HR1MJDCKLH4CD88ELEGDUE5J4UA3QGZZ
```

#### Password.txt

```
9XF4AF7M; 123456; 111111
W472TJXH; 123456; 111111
```

Single System	
OOB	<pre>saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SecureEraseDisk [--current_password &lt;current password&gt;   -- cur_pw_file &lt;current password file path&gt;] --file &lt;filename&gt; --precheck saa -i &lt;IP or host name&gt; -u &lt;username&gt; -p &lt;password&gt; -c SecureEraseDisk [--current_password &lt;current password&gt;   -- cur_pw_file &lt;current password file path&gt;] --file &lt;filename&gt; --action &lt;action&gt; [--reboot [--post_complete]]</pre>
In-Band	<pre>saa -c SecureEraseDisk [--current_password &lt;current password&gt;   -- cur_pw_file &lt;current password file path&gt;] --file &lt;filename&gt; --precheck saa -c SecureEraseDisk [--current_password &lt;current password&gt;   -- cur_pw_file &lt;current password file path&gt;] --file &lt;filename&gt; --action &lt;action&gt; [--reboot]</pre>
Multiple Systems	
OOB	<pre>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SecureEraseDisk [--current_password &lt;current password&gt;   -- cur_pw_file &lt;current password file path&gt;] --file &lt;filename&gt; --precheck saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c SecureEraseDisk [--current_password &lt;current password&gt;   --</pre>

---

	<code>cur_pw_file &lt;current password file path&gt;] --file &lt;filename&gt; --action &lt;action&gt; [--reboot [--post_complete]]</code>
--	-----------------------------------------------------------------------------------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SecureEraseDisk --file Password.txt --precheck
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SecureEraseDisk --file Password.txt --action SetPassword --reboot
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
SecureEraseDisk --file Password.txt --action SecurityErase --reboot
```

**In-Band:**

```
[SAA_HOME]# ./saa -c SecureEraseDisk --file PSID.txt --precheck
```

```
[SAA_HOME]# ./saa -c SecureEraseDisk --file Password.txt --action
SecurityErasePWD --reboot
```

```
[SAA_HOME]# ./saa -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 NumberS45RNE0M600194
 Password StatusNOT INSTALLED
 Security ModeSAT3 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.
```

### Multiple Systems 00B:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseDisk --
file psid.txt --precheck
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SecureEraseDisk --
file psid.txt --action SetPassword --reboot
```

```
[SAA_HOME]# ./saa -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 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:

- 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 the BIOS to provide more information, but when loaded, the storage cannot be securely erased by the 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.
- An additional password cannot be assigned to the HDD with a password already 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 must 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
- 

#### 5.18.10.1. 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.
  - **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:** Changes the HDD password.
  - **ClearPassword:** 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.

#### 5.18.10.2. 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, which includes all unmapped hard disks. Note that the PSID.txt is only supported by TGC devices.

```
./saa -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file PSID.txt --precheck
```

```
./saa -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file Password.txt --precheck
```

```
Managed system.....192.168.34.56
[HDD]
 Serial Number9XF4AF7M
 Password StatusNOT INSTALLED
 Security ModeSAT3 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.....33 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.

```
./saa -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file PSID.txt --
action SecurityErasePSID --reboot --post_complete
```

```
./saa -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file
Password.txt --action SecurityErasePWD --reboot
```

**The console output with --post\_complete option contains the following information.**

```
.....
Status: Enable Secure Erase Automation.

Status: The managed system 192.168.34.56 is rebooting.

.....
.....
.....Done
.....
.....
.....
Status: Security erase for HDD is set for 192.168.34.56

Status: The managed system 192.168.34.56 is waiting for POST complete

Status: PCIResourceConfigStarted

.....
.....
Status: MemoryInitializationStarted

.....
Status: PCIResourceConfigStarted

.....
.....
Status: MemoryInitializationStarted

.....
Status: MemoryInitializationStarted

.....
.....
Status: PCIResourceConfigStarted
```

---

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

**The console output without `--post_complete` option contains the following information.**

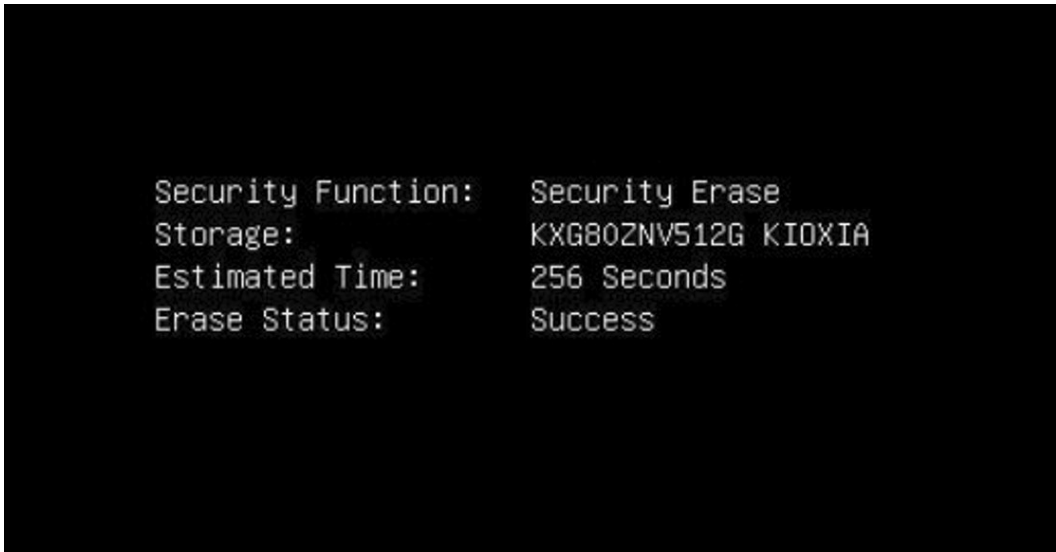
```
.....
Status: Enable Secure Erase Automation.

Status: The managed system 192.168.34.56 is rebooting.

.....
.....Done
.....
.....
.....
Status: Security erase for HDD is set for 192.168.34.56

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

3. The monitoring result of the managed system appears.



```
Security Function: Security Erase
Storage: KXG80ZNV512G KIOXIA
Estimated Time: 256 Seconds
Erase Status: Success
```

After the task is complete, use the SAA `GetCurrentBiosCfg` command to check the result through BIOS configurations. Find the status code in the configuration file in xml format by searching for “Last Status Code.” A status code of zero indicates that the





---

### 5.18.10.3. Setting Up 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.

```
./saa -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file
Password.txt --precheck
```

```
Managed system.....192.168.34.56
[HDD]
 Serial Number9XF4AF7M
 Password StatusNOT INSTALLED
 Security ModeSAT3 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.....33 Minutes
Please check the PreCheckFile for the mismatched HDDs.
```

2. Run the command to set an HDD password.

```
./saa -i IP -u ADMIN -p PASSWORD -c SecureEraseDisk --file
Password.txt --action SetPassword --reboot
```

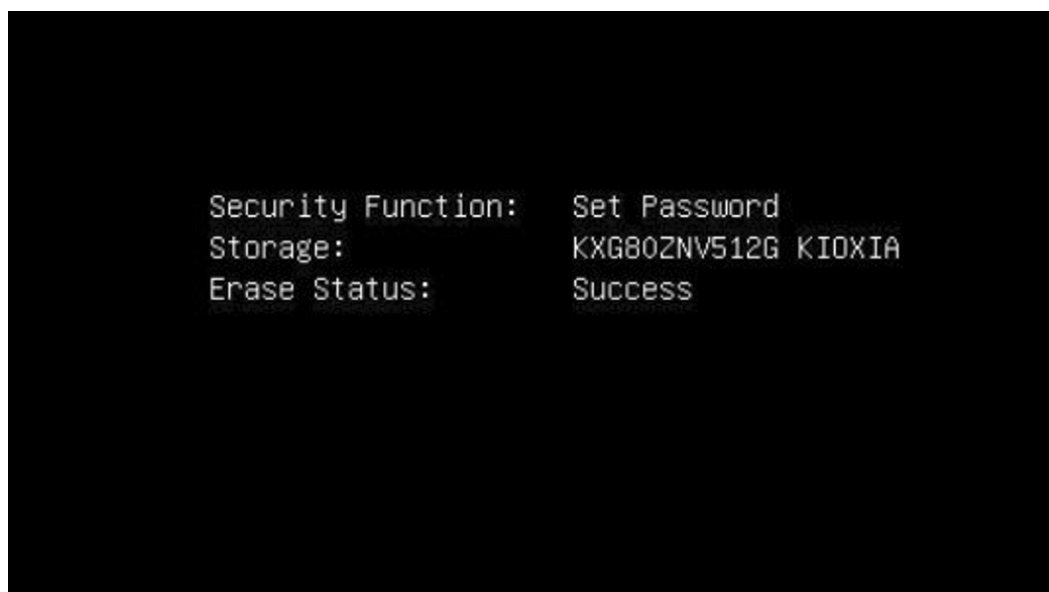
```
.....
Status: Enable Secure Erase Automation.

Status: The managed system 192.168.34.56 is rebooting.

.....
.....
.....Done
.....
.....
.....
Status: The HDD password is set for 192.168.34.56
```

WARNING: Without option --post\_complete, please manually confirm the managed system is POST complete before executing next action.

3. The monitoring result of the managed system appears.



4. After the task is complete, to check the execution result, run the SAA GetCurrentBiosCfg command (see 5.4.3 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 successful. For non-zero status codes, please refer to Appendix D - Status Codes in [UEFI Specification 2.8](#).

### 5.18.11. Getting CPU ERoT Firmware Image Information

Use the "GetCpuERoTInfo" command to get the ERoT CPU firmware image information of NVIDIA MGX™ systems from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetCpuERoTInfo
In-Band	saa -l Redfish_HI -u <username> -p <password> -c GetCpuERoTInfo
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c

---

	GetCpuERoTInfo
--	----------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetCpuERoTInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
 [CPU 0]
 ERoT version.....01.03.0103.0000_n01
 [CPU 1]
 ERoT version.....01.03.0103.0000_n01
```

**In-Band Redfish Host Interface:**

```
[SAA_HOME]# ./saa -c GetCpuERoTInfo -I Redfish_HI -u ADMIN -p ADMIN
```

**The console output contains the following information.**

```
Managed system.....169.254.3.254
 [CPU 0]
 ERoT version.....01.03.0103.0000_n01
 [CPU 1]
 ERoT version.....01.03.0103.0000_n01
```

**Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetCpuERoTInfo
```

```
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.

---

### 5.18.12. Updating CPU ERoT Firmware Image

Use the “UpdateCpuERoT” command with the CPU ERoT firmware image CPU\_ERoT.fwpkg to run SAA on NVIDIA MGX™ systems to update the CPU ERoT of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateCpuERoT --file <filename>
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateCpuERoT -file <filename>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateCpuERoT --file <filename>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateCpuERoT --file CPU_ERoT.fwpkg
```

#### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c UpdateCpuERoT --file CPU_ERoT.fwpkg
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateCpuERoT --file CPU_ERoT.fwpkg
```

```
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.

### 5.18.13. Managing CPU ERoT RoT Functions

The “CpuERotManage” command supports the following features on NVIDIA MGX™ Systems:

- **Getting Information on CPU ERoT**  
Use the “CpuERotManage” command with the “--action GetInfo” option to retrieve information about the active ERoT CPU and the golden ERoT CPU.
- **Updating the Golden Image**  
Use the “CpuERotManage” command with the “--action UpdateGolden” option to replace the golden image with an active ERoT CPU firmware.
- **Recovering ERoT CPU**  
Use the “CpuERotManage” command with the “--action Recover” option to recover ERoT CPU from the backup image or the golden image. By priority, the managed system recovers ERoT CPU from the backup image. If the backup image is corrupted, it will then recover from the golden image.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CpuERotManage --action <action>
In-Band	saa -I Redfish_HI -u <username> -p <password> -c CpuERotManage - -action <action>
Multiple Systems	
OOB	saa -I <system list file> [-u <username> -p <password>] -c CpuERotManage --action <action>

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CpuERotManage
--action GetInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
CPU ERoT 0 version.....01.03.0103.0000_n01
Golden CPU ERoT version.....01.03.0103.0000_n01
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CpuERotManage
--action UpdateGolden
```

**The console output contains the following information.**

```
.....
Status: System is backing up current FW as golden image. Please wait for 2
minutes.
.....
.....
Done
Status: Please check golden FW version for result.
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CpuERotManage
--action Recover
```

**The console output contains the following information.**

```
.....
Status: System is recovering ERoT CPU firmware image. Please wait for 2 minutes.
.....
.....
Done
Status: Please check golden FW version for result.
```

**In-Band :**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c CpuERotManage --
action UpdateGolden
```

**The console output contains the following information.**

```

.....
Status: System is backing up current FW as golden image. Please wait for 2
minutes.
.....
.....
Done
Status: Please check golden FW version for result.

```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c CpuERotManage --
action UpdateGolden
```

```

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.

## 5.18.14. Managing Motherboard FPGA RoT Functions

The “FpgaRotManage” command supports the following features on NVIDIA MGX™ Systems:

- Getting Information on Motherboard FPGA**  
 Use the “FpgaRotManage” command with the option “--action GetInfo” to retrieve information on active FPGA and golden FPGA.
- Updating the Golden Image**  
 Use the “FpgaRotManage” command with the “--action UpdateGolden” option to replace the golden image with an active FPGA firmware.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c FpgaRotManage --action <action>
In-Band	saa -I Redfish_HI -u <username> -p <password> -c FpgaRotManage -



	-action <action>
<b>Multiple Systems</b>	
OOB	saa -l <system list file> [-u <username> -p <password>] -c FpgaRotManage --action <action>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c FpgaRotManage
--action GetInfo
```

**The console output contains the following information.**

```
Managed system.....192.168.34.56
 FPGA version.....0.78
 Golden FPGA version.....0.78
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c FpgaRotManage
--action UpdateGolden
```

**The console output contains the following information.**

```
.....
Status: System is backing up current FW as golden image. Please wait for 2
minutes.
.....
.....
Done
Status: Please check golden FW version for result.
```

#### In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c FpgaRotManage --
action UpdateGolden
```

**The console output contains the following information.**

```

.....
Status: System is backing up current FW as golden image. Please wait for 2
minutes.
.....
.....
Done
Status: Please check golden FW version for result.

```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c FpgaRotManage --
action UpdateGolden
```

```

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.

### 5.18.15. Getting GPU External RoT (ERoT) Firmware Image Information

Use the “GetGpuERoTInfo” command to get the External RoT (ERoT) GPU firmware image information of NVIDIA MGX™ systems from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetGpuERoTInfo
In-Band	saa -l Redfish_HI -u <username> -p <password> -c GetGpuERoTInfo
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetGpuERoTInfo

Example:

**OOB:**

---

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetGpuERoTInfo
```

The console output contains the following information.

```
Managed system.....192.168.34.56
 [GPU 0]
 ERoT version.....01.03.0103.0000_n01
```

#### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -c GetGpuERoTInfo -I Redfish_HI -u ADMIN -p ADMIN
```

The console output contains the following information.

```
Managed system.....169.254.3.254
 [GPU 0]
 ERoT version.....01.03.0103.0000_n01
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetGpuERoTInfo
```

```
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.

### 5.18.16. Getting SPDM Measurement Information

Use the “GetSpdmInfo” command to get and read the SPDM Measurement information of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSpdmInfo --item <item_name> [--showall]

In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetSpdmInfo --item <item_name> [--showall]
<b>Multiple Systems</b>	
OOB	saa -I < system list file > [-u <username> -p <password>] -c GetSpdmInfo --item <item_name> [--showall]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetSpdmInfo --item CPU
```

The console output contains the following information if the platform is supported to manage SPDM Measurement devices.

```
Managed system.....172.30.102.144
Item.....CPU
MeasurementSummary.....19E71EA9A1DD8CB7CD352A636C54CE30
 A8455B7EF494C83EC213340C6BCD7003
 D8BC11B671D73146E7B09F33FDB22C08
Measurement(01).....01010700830400000000003
Measurement(02).....020107008304004E564300
Measurement(03).....03010400830100FF
Measurement(04).....04013300013000F3B4B4DD0B66A1A529
 83177E71C697904458ED0452C6431C26
 5BE4FA9529D0A1E9983E864FCC74B665
 88E66C5E53BAE9
```

#### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetSpdmInfo --item CPU --showall
```

The console output contains the following information if the platform is supported to manage SPDM Measurement devices.

```
Managed system.....169.254.3.254
MeasurementSummary.....B4CBFE417CFFF035582F075F970EFA59
 B9DB5231CED16E4EA5191FF60EE4935A
```



---

- **Getting Information on CMM**

Use the “CmmRotManage” command with the “--action GetInfo” option to retrieve information on active CMM, backed-up CMM and golden CMM.

- **Updating the Golden Image**

Use the “CmmRotManage” command with the “--action UpdateGolden” option to replace the golden image with an active CMM firmware.

- **Recovering CMM**

Use the “CmmRotManage” command with the “--action Recover” option to recover CMM from the backup image or the golden image. By priority, the managed system recovers CMM from the backup image. If the backup image is corrupted, it will then recover from the golden image.

- **Downloading CMM Evidence**

Use the “CmmRotManage” command with the “--action DownloadEvidence” option to download CMM evidence.



**Notes:**

- This command is only supported on Blade system with CMM AST2600.
- CMM will be disconnected while updating the golden image and recovering the firmware. Use the “GetMaintenEventLog” command to check the result afterwards. For details, see 5.6.3 *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.
- The “DownloadEvidence” action is only available after automatic or manual CMM recovery.
- The CMM evidence is a compressed gzip file.

---

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CmmRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]]
Multiple Systems	

---

OOB	<code>saa -l &lt;system list file&gt; [-u &lt;username&gt; -p &lt;password&gt;] -c CmmRotManage --action &lt;action&gt; [--file &lt;evidence.bin.gz&gt; [--overwrite]]</code>
-----	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Example:

**OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CmmRotManage -
-action GetInfo
```

**The console output contains the following information.**

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

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CmmRotManage -
-action DownloadEvidence --file evidence.bin.gz
```

**The console output contains the following information.**

```
.....
Start generating CMM evidence.
.....Done
Start downloading CMM evidence.....Done
CMM evidence file "evidence.bin.gz" is created.
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CmmRotManage -
-action UpdateGolden
```

**The console output contains the following information.**

```
.....
Status: System is backing up current FW as golden image and CMM will be offline
for 6 minutes.
.....
.....
```

---

```
Done
Status: Please check Maintenance Event log for result.
```

### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c CmmRotManage --
action UpdateGolden
```

```
SList.txt:
192.168.34.56
192.168.34.57
```

## 5.19. FPGA Management

### 5.19.1. Getting Motherboard FPGA Firmware Image Information

Use the “GetMotherboardFpgaInfo” command to get the motherboard FPGA firmware image and its corresponding information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetMotherboardFpgaInfo [--file <filename>]
In-Band	saa -l Redfish_HI -u <username> -p <password> -c GetMotherboardFpgaInfo [--file <filename>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetMotherboardFpgaInfo [--file <filename>]

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetMotherboardFpgaInfo --file FPGA.bin
```

The console output contains the following information.



```
Managed system.....192.168.34.56
 Motherboard FPGA version.....F3.74.23
Local FPGA image file.....FPGA.bin
 FPGA version.....F3.74.23
```

#### In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c
GetMotherboardFpgaInfo
```

The console output contains the following information.

```
Managed system.....169.254.3.254
 Motherboard FPGA version.....F3.74.23
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetMotherboardFpgaInfo
```

```
SList.txt:
 192.168.34.56
 192.168.34.57
```

If the execution “Status” field for the managed system is SUCCESS, the FPGA information of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

### 5.19.2. Updating Motherboard FPGA Firmware Image

Use the “UpdateMotherboardFpga” command with the motherboard FPGA firmware image FPGA.bin to run SAA on NVIDIA MGX™ systems to update the motherboard FPGA of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c

	UpdateMotherboardFpga --file <filename> --reboot
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateMotherboardFpga --file <filename> --reboot
<b>Multiple Systems</b>	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMotherboardFpga --file <filename> --reboot

Example:

#### **OOB:**

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateMotherboardFpga --file FPGA.bin --reboot
```

#### **In-Band through Redfish Host Interface:**

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
UpdateMotherboardFpga --file FPGA.bin --reboot
```

#### **Multiple Systems OOB:**

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
UpdateMotherboardFpga --file FPGA.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.

## **5.20. MCU Management**

### **5.20.1. Getting Motherboard MCU Firmware Image Information**

Use the “GetMotherboardMcuInfo” command to get the motherboard MCU firmware image information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetMotherboardMcuInfo
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetMotherboardMcuInfo
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetMotherboardMcuInfo

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
GetMotherboardMcuInfo
```

```
Managed system.....192.168.34.56
Motherboard MCU version.....FF.11.07
```

#### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
GetMotherboardMcuInfo
```

```
Managed system.....169.254.3.254
Motherboard MCU version.....FF.11.07
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
GetMotherboardMcuInfo
```

```
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.

### 5.20.2. Updating Motherboard MCU Firmware Image

Use the “UpdateMotherboardMcu” command with the motherboard MCU firmware image MBD\_MCU.bin to run SAA to update the motherboard MCU of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateMotherboardMcu --file <filename> --reboot [--post_complete]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateMotherboardMcu --file <filename> --reboot
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMotherboardMcu --file <filename>

Example:

#### OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateMotherboardMcu --file MBD_MCU.bin --reboot --post_complete
```

#### In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
UpdateMotherboardMcu --file MBD_MCU.bin --reboot
```

#### Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
UpdateMotherboardMcu --file MBD_MCU.bin
```

```
SList.txt:
192.168.34.56
```

---

192.168.34.57

The execution progress for the managed system will be continuously updated to the “Execution Message” section of the managed system in the created log file.

---

## Appendix A. SAA Exit Codes

Exit Code Number	Description
0	Successful
Others	Failed
<b>GROUP1 (1~30) Command line parsing check failed</b>	
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
<b>GROUP2 (31~59) Resource management error</b>	
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
<b>GROUP3 (60~79) File parsing errors</b>	
61	Utility internal error
63	Invalid firmware flash ROM
<b>GROUP4 (80~99) IPMI operation errors</b>	
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
<b>GROUP5 (100~119) In-band operation errors</b>	
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
<b>GROUP6 (120~199) IPMI communication errors</b>	
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
201	Invalid API response
247	Remote SSH execution failed
248	Minimum SAA version is required
249	Special action is required
250	Managed firmware error
251	Rooted exception
252	Nested exception
253	Known limitation
254	Manual steps are required



**Note:** 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.

---

## Appendix B. Management Interface and License Requirements

[ Group ] Command	Management Interface Supported		Execution Mode File-based (F) / Command-based (C)	Minimum Required License for Managed System	Note
	Out-Of-Band	In-Band			
	(Remote)	(Local)			
[ License Management ]					
ActivateProductKey	Yes	Yes	F + C	No license required	
QueryProductKey	Yes	Yes	C	No license required	
CpuOnDemand	Yes	Yes	C	SFT-DCMS-SINGLE	
[ Health Management ]					
CheckOOBSupport	Yes	Yes	C	No license required	

CheckAssetInfo	Yes	No	C	No license required	
CheckSystemUtilization	Yes	No	C	<b>SFT-OOB-LIC</b>	
CheckSensorData	Yes	No	C	No license required	
ServiceCalls	Yes	Yes	F + C	<b>SFT-DCMS-SINGLE + SFT-DCMS-SVC-KEY</b>	
SystemPFA	Yes	Yes	C	<b>SFT-OOB-LIC</b>	
MemoryHealthCheck	Yes	Yes	C	<b>SFT-OOB-LIC</b>	
ChassisIntrusion	Yes	Yes	C	No license required	
AlertManage	Yes	Yes	C	No license required	
SuperDiag	Yes	Yes	F + C	No license required	
SendDiagInterrupt	Yes	Yes	C	No license required	
MonitorCDUStatus	Yes	No	F + C	No license required	
TasManage	Yes	Yes	C	No license required	

CheckSelfTest	Yes	Yes	C	SFT- OOB- LIC	
HDTService	Yes	Yes	C	SFT- DCMS- SINGLE	
<b>[ System Management ]</b>					
GetFruInfo	Yes	Yes	F + C	No license required	
RestoreFruInfo	Yes	Yes	F	No license required	
ChangeFruInfo	Yes	Yes	C	No license required	
GetSystemInfo	Yes	Yes	C	No license required	
GetSystemCfg	Yes	Yes	F + C	SFT- OOB- LIC	
ChangeSystemCfg	Yes	Yes	F	SFT- OOB- LIC	
GetFanMode	Yes	Yes	C	No license required	
SetFanMode	Yes	Yes	C	No license required	
LocateServerUid	Yes	Yes	C	No license required	
GetFirmwareInventoryInfo	Yes	Yes	C	No license required	
ClearCMOS	Yes	Yes	C	No license	

				required	
<b>[ BIOS Management ]</b>					
GetBiosInfo	Yes	Yes	C	No license required	
UpdateBios (without --preserve_setting)	Yes	Yes	C	No license required	
UpdateBios (with --preserve_setting)	Yes	Yes	C	No license required	<b>SFT-OOB-LIC is required for X12 3rd Generation Intel® Xeon® Scalable processors with Intel® C620 Series Chipsets</b>
GetDefaultBiosCfg	Yes	Yes	F + C	<b>SFT-OOB-LIC</b>	
GetCurrentBiosCfg	Yes	Yes	F + C	<b>SFT-OOB-LIC</b>	
ChangeBiosCfg	Yes	Yes	F	<b>SFT-OOB-LIC</b>	<b>SFT-DCMS-SINGLE is required for some configuration items</b>
LoadDefaultBiosCfg	Yes	Yes	C	<b>SFT-OOB-LIC</b>	
SetBiosPassword	Yes	Yes	F + C	<b>SFT-OOB-LIC</b>	
GetDmiInfo	Yes	Yes	F	<b>SFT-OOB-LIC</b>	
ChangeDmiInfo	Yes	Yes	F	<b>SFT-OOB-LIC</b>	
EditDmiInfo	Yes	Yes	F	<b>SFT-OOB-LIC</b>	

EraseOAKey	No	Yes	C	No license required	
GetScplInfo	Yes	No (Yes for ARM64)	C	No license required	
UpdateScp	Yes	No (Yes for ARM64)	C	No license required	
GetFixedBootCfg	Yes	Yes	F + C	SFT-DCMS-SINGLE	
ChangeFixedBootCfg	Yes	Yes	F	SFT-DCMS-SINGLE	
GetBootOption	Yes	Yes	C	No license required	
SetBootOption	Yes	Yes	C	No license required	
SetHttpBoot	Yes	Yes	F + C	SFT-OOB-LIC	SFT-DCMS-SINGLE is required for TLS upload configuration
GetBiosPostCode	Yes	No	C	No license required	
<b>[ BMC Management ]</b>					
GetBmcInfo	Yes	Yes	C	No license required	
UpdateBmc	Yes	Yes	C	No license required	
GetBmcCfg	Yes	Yes	F + C	SFT-OOB-LIC	

ChangeBmcCfg	Yes	Yes	F	<b>SFT- OOB- LIC</b>	
GetBmcLANCfg	Yes	Yes	F + C	No license required	
ChangeBmcLANCfg	Yes	Yes	F	No license required	
SetBmcPassword	Yes	Yes	F + C	No license required	
GetKcsPriv	Yes	Yes	C	<b>SFT- OOB- LIC</b>	
SetKcsPriv	Yes	No	C	<b>SFT- OOB- LIC</b>	
LoadDefaultBmcCfg	Yes	Yes	C	No license required	
GetBmcUserList	Yes	Yes	C	<b>SFT- OOB- LIC</b>	
SetBmcUserList	Yes	Yes	C	<b>SFT- OOB- LIC</b>	
TimedBmcReset	Yes	Yes	C	No license required	
BootStrappingAccount	Yes	Yes	C	No license required	
RmcpManage	Yes	Yes	C	<b>SFT- OOB- LIC</b>	
GetSessionInfo	Yes	No	C	No license required	

BmcHostName	Yes	Yes	C	No license required	
ManageRHI	Yes	Yes	C	No license required	
SnmpManage	Yes	Yes	C	No license required	
BmcWatchDog	Yes	Yes	C	No license required	
FindBmcDevices	No	Yes	F + C	No license required	
<b>[ System Event Log ]</b>					
GetEventLog	Yes	Yes	C	No license required	
ClearEventLog	Yes	Yes	C	No license required	<b>SFT-OOB-LIC is required for --clear_bios_eventlog option</b>
GetMaintenEventLog	Yes	Yes	C	No license required	
ClearMaintenEventLog	Yes	Yes	C	No license required	
GetHostDump	Yes	Yes	F + C	<b>SFT-DCMS-SINGLE</b>	
<b>[ CMM Management ]</b>					
GetCmmInfo	Yes	Yes	C	No license required	
UpdateCmm	Yes	No	C	No license required	



GetCmmCfg	<b>Yes</b>	No	F + C	No license required	
ChangeCmmCfg	<b>Yes</b>	No	F	No license required	
SetCmmPassword	<b>Yes</b>	No	F + C	No license required	
LoadDefaultCmmCfg	<b>Yes</b>	No	C	No license required	
GetBbpInfo	<b>Yes</b>	No	C	No license required	
UpdateBbp	<b>Yes</b>	No	C	No license required	
GetBladePowerStatus	<b>Yes</b>	No	C	No license required	
SetBladePowerAction	<b>Yes</b>	No	C	No license required	
ProfileManage	<b>Yes</b>	No	C	No license required	
GetBladeSwitchInfo	<b>Yes</b>	No	F + C	No license required	
UpdateBladeSwitch	<b>Yes</b>	No	F + C	No license required	
RebootBladeSwitch	<b>Yes</b>	No	C	No license required	
BladePsuManage	<b>Yes</b>	<b>Yes</b>	C	No license required	

BladeSummary	Yes	Yes	C	No license required	
GetCmmUserList	Yes	Yes	C	SFT-OOB-LIC	
SetCmmUserList	Yes	Yes	C	SFT-OOB-LIC	
UpdateDummySwitch	Yes	No	F + C	No license required	
<b>[ Storage Management ]</b>					
GetRaidControllerInfo	Yes	Yes	C	SFT-DCMS-SINGLE	
UpdateRaidController	Yes	Yes	C	SFT-DCMS-SINGLE	
GetRaidCfg	Yes	Yes	F + C	SFT-DCMS-SINGLE	
ChangeRaidCfg	Yes	Yes	F	SFT-DCMS-SINGLE	
GetSataInfo	Yes	No	C	SFT-OOB-LIC	
GetNvmeInfo	Yes	Yes	C	No license required	
ControlNVMe	Yes	Yes	C	No license required	
GetPMemInfo	Yes	Yes	C	SFT-DCMS-SINGLE	
UpdatePMem	Yes	Yes	C	SFT-DCMS-	

				<b>SINGLE</b>	
GetVROCCfg	<b>Yes</b>	<b>Yes</b>	F + C	<b>SFT- OOB- LIC</b>	
ChangeVROCCfg	<b>Yes</b>	<b>Yes</b>	F	<b>SFT- OOB- LIC</b>	
GetSmartData	<b>Yes</b>	<b>Yes</b>	C	No license required	
GetSasExpanderInfo	<b>Yes</b>	<b>Yes</b>	C	<b>SFT- DCMS- SINGLE</b>	
UpdateSasExpander	<b>Yes</b>	<b>Yes</b>	C	<b>SFT- DCMS- SINGLE</b>	
<b>[ PSU Management ]</b>					
GetPsuInfo	<b>Yes</b>	<b>Yes</b>	C	<b>SFT- OOB- LIC</b>	
UpdatePsu	<b>Yes</b>	<b>Yes</b>	C	<b>SFT- DCMS- SINGLE</b>	
GetPowerStatus	<b>Yes</b>	<b>Yes</b>	C	No license required	
SetPowerAction	<b>Yes</b>	<b>Yes</b>	C	No license required	
DcmiManage	<b>Yes</b>	<b>Yes</b>	C	No license required	
PowerPolicy	<b>Yes</b>	<b>Yes</b>	C	No license required	
GetAcpiPowerStatus	<b>Yes</b>	<b>Yes</b>	C	No license required	

GetAiomStandbyPower	Yes	No	C	No license required	
SetAiomStandbyPower	Yes	No	C	No license required	
GetPsFruInfo	Yes	Yes	C	No license required	
<b>[ PCIeSwitch Management ]</b>					
GetPCleSwitchInfo	No	Yes	C	No license required	
UpdatePCleSwitch	No	Yes	C	No license required	
<b>[ Applications ]</b>					
GetUsbAccessMode	No	Yes	C	<b>SFT-DCMS-SINGLE</b>	
SetUsbAccessMode	No	Yes	C	<b>SFT-DCMS-SINGLE</b>	
RawCommand	Yes	Yes	C	No license required	
KmsManage	Yes	Yes	F + C	<b>SFT-OOB-LIC</b>	<b>SFT-DCMS-SINGLE is required for TLS upload configuration</b>
RedfishApi	Yes	Yes	C	No license required	
RemoteExec	No	<b>Yes (Remote Only)</b>	F + C	No license required	
RemoteConsole	Yes	No	C	No license required	

RemoteScreenshot	<b>Yes</b>	No	F	SFT-DCMS-SINGLE	
RemoteKeyboard	<b>Yes</b>	No	F	SFT-DCMS-SINGLE	
Sol	<b>Yes</b>	No	C	No license required	
FindBmcDevices	<b>No</b>	Yes	C/F	No license required	
FoundBmcDevices	No	<b>Yes</b>	F + C	No license required	
Shell	<b>Yes</b>	No	C	No license required	
Prompt	No	<b>Yes</b>	C	No license required	
<b>[ GPU Management ]</b>					
GetGpuInfo	<b>Yes</b>	<b>Yes</b>	C	<b>SFT-DCMS-SINGLE</b>	
UpdateGpu	<b>Yes</b>	<b>Yes</b>	C	<b>SFT-DCMS-SINGLE</b>	
DiagGpuStatus	<b>Yes</b>	<b>Yes</b>	C	<b>SFT-OOB-LIC</b>	
GetGpuLog	<b>Yes</b>	<b>Yes</b>	C	<b>SFT-DCMS-SINGLE</b>	
<b>[ CPLD Management ]</b>					
GetCpldInfo	<b>Yes</b>	<b>Yes</b>	C	No license required	

UpdateCpld	Yes	Yes	C	No license required	
GetSwitchboardCpldInfo	Yes	Yes	C	No license required	
UpdateSwitchboardCpld	Yes	Yes	C	No license required	
GetFanboardCpldInfo	Yes	Yes	C	No license required	
UpdateFanboardCpld	Yes	Yes	C	No license required	
GetBackplaneCpldInfo	Yes	Yes	C	No license required	
UpdateBackplaneCpld	Yes	No	C	No license required	
GetAipCpldInfo	Yes	Yes	C	No license required	
UpdateAipCpld	Yes	Yes	C	No license required	
GetAomboardCpldInfo	Yes	Yes	C	<b>SFT-DCMS-SINGLE</b>	
UpdateAomboardCpld	Yes	Yes	C	<b>SFT-DCMS-SINGLE</b>	
GetMiscCpldInfo	Yes	Yes	C	No license required	
UpdateMiscCpld	Yes	Yes	C	No license required	

GetMidplaneSbbCpldInfo	Yes	Yes	C	No license required	
UpdateMidplaneSbbCpld	Yes	No	C	No license required	
GetNICCpldInfo	Yes	Yes	C	<b>SFT-DCMS-SINGLE</b>	
UpdateNICCpld	Yes	Yes	F	<b>SFT-DCMS-SINGLE</b>	
GetTransitionboardCpldInfo	Yes	Yes	C	No license required	
UpdateTransitionboardCpld	Yes	No	C	No license required	
<b>[ NIC Management ]</b>					
GetAocNICInfo	Yes	Yes	C	<b>SFT-DCMS-SINGLE</b>	
UpdatetAocNIC	Yes	Yes	C	<b>SFT-DCMS-SINGLE</b>	
<b>[ Multi-Node Management ]</b>					
GetTpInfo	Yes	Yes	F + C	No license required	
ChangeTpInfo	Yes	Yes	F	No license required	
GetMultinodeEcInfo	Yes	Yes	C	No license required	
UpdateMultinodeEc	Yes	Yes	C	No license required	

[ VM Management ]					
MountIsoImage	Yes	Yes	C	SFT-OOB-LIC	
UnmountIsoImage	Yes	Yes	C	SFT-OOB-LIC	
MountFloppyImage	Yes	Yes	C	SFT-OOB-LIC	
UnmountFloppyImage	Yes	Yes	C	SFT-OOB-LIC	
GetVmInfo	Yes	Yes	C	SFT-OOB-LIC	
VmManage	Yes	Yes	C	SFT-OOB-LIC	
VMShell	Yes	No	C	SFT-DCMS-SINGLE	
[ NM Management ]					
NmMeManage	Yes	Yes	C	No license required	
GeneralNmManage	Yes	Yes	C	No license required	
NmCpuManage	Yes	Yes	C	No license required	
NmCupsManage	Yes	Yes	C	No license required	
BmcNmManage	Yes	Yes	C	No license required	



[ Security Management ]					
BiosRotManage	Yes	Yes	C	No license required	SFT-DCMS-SINGLE is required for Recover and DownloadEvidence actions
BmcRotManage	Yes	Yes	C	No license required	SFT-DCMS-SINGLE is required for Recover and DownloadEvidence actions.
CpldRotManage	Yes	Yes	C	No license required	
SecureBootManage	Yes	Yes	F + C	SFT-DCMS-SINGLE	
GetLockdownMode	Yes	Yes	C	SFT-DCMS-SINGLE	
SetLockdownMode	Yes	No	C	SFT-DCMS-SINGLE	
Attestation	Yes	Yes	F + C	SFT-DCMS-SINGLE	Both SFT-DCMS-SINGLE and SFT-SDDC-SINGLE are required for action Compare.
SecureEraseDisk	Yes	Yes	F + C	SFT-DCMS-SINGLE	
SecureEraseRaidHdd	Yes	Yes	C	SFT-DCMS-SINGLE	
TpmProvision	Yes	No	C	SFT-OOB-LIC	
GetTpmInfo	Yes	Yes	C	SFT-OOB-LIC	

TpmManage	Yes	Yes	C	<b>SFT-OOB-LIC</b>	
GetCpuERoTInfo	Yes	Yes	C	No license required	
UpdateCpuERoT	Yes	Yes	C	No license required	
CpuERoTManage	Yes	Yes	C	No license required	
FpgaRotManage	Yes	Yes	C	No license required	
GetCpuERoTInfo	Yes	Yes	C	No license required	
GetSPDMInfo	Yes	Yes	C	No license required	
CmmRotManage	Yes	Yes	C	No license required	<b>SFT-DCMS-SINGLE is required for Recover and DownloadEvidence actions.</b>
<b>[ FPGA Management ]</b>					
GetMotherboardFpgaInfo	Yes	Yes	C	No license required	
UpdateMotherboardFpga	Yes	No	C	No license required	
<b>[ MCU Management ]</b>					
GetMotherboardMcuInfo	Yes	Yes	C	No license required	
UpdateMotherboardMcu	Yes	Yes	C	No license	

				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 further actions from SAA 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.
- When assigning the SAA arguments in command line, please be aware of the escape characters.

### License Management

- When activating JSON format key in Windows, the JSON key string cannot contain any spaces.

### Health Management

- You cannot access any cache files on mounted file systems with the ServiceCalls command.

### BIOS Management

- The OOB UpdateBios command support on X13 and later motherboards depends on each hardware, BIOS and BMC supportability for motherboards that implement clientME such as (includes but not limited to) X13Sax series.
- With the Server ME embedded on the Supermicro system, the execution of the in-band command "UpdateBios" might fail when the Client ME driver (MEI64) 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).
- 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.
- 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.
- 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.

### **Power Management**

- The UpdatePsu command only supports PSU "PWS-2K04A-1R" and "PWS-2K20A-1R."
- The UpdatePsu command does not support multiple OOB usages.

### **PCleSwitch Management**

- All PCIe Switch management commands are for In-Band use only.
- All PCIe Switch management commands only support H12DGQ-NT6 with Broadcom PCIe Switch Gen4 Series chipsets and X12DSC-6 with Microchip PCIe Switch Gen4 Series chipsets platforms.

### **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.

### **VM Management**

- If the device is mounted by iKVM, the device can only be unmounted by iKVM.

---

## Security Management

- While executing the UpdateBIOS/In-Band TpmManage commands, manual steps are required under some special cases. Instructions will be provided to continue these commands.

---

## Appendix D. Third-Party Software

The following open-source libraries are used in SAA package:

Program	Library	Version	License
saa	simpleopt	3.5	MIT
saa	pugixml	1.2	MIT
saa	Libcurl	8.4.0	MIT
saa	openssl	3.0.11	OpenSSL
saa	CryptoPP	5.6.2	Boost 1.0
saa	EDK2 Compress/ Decompress	EDK2	BSD
saa	Jsoncpp	1.8.4	MIT
phymem.sys/pmdll.d	phymem	2.7.0.3	CPOL
saa	ncurses	6.1	MIT
saa	PDCurses	3.6	MIT
ExternalData/tui.fnt	Terminus Font	N/A	OFL 1.1
saa	rapidcsv	8.6	MIT
saa	UEFITool	NE alpha 58/ 0.21.5	BSD 2-Clause
saa	Sqlite	3.42.0	public domain
saa	Sqlite_orm	V1.6	BSD 3-Clause
saa	CxxUrl	V0.1	MIT
saa	Libssh2	1.11.0	BSD 3-Clause
saa	Acpica	20191018	BSD
saa	Isocline	1.0.2	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>
<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

SAA 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, SAA will load the file from system and upload it to BIOS. The following example is the setting of TLS upload:

### E.5.1.1 TLS Certificate

```

" <Setting name="Enroll HTTPS Boot TLS Certificate" type="String">
 <Information>
 <MinSize>0</MinSize>
 <MaxSize>255</MaxSize>
 <DefaultString></DefaultString>

```

---

```
<Help><![CDATA[Enroll HTTPS Boot TLS Certificate with type .cer,.der,.crt,.pem]]>
</Help>
<AllowingMultipleLine>False</AllowingMultipleLine>
<LicenseRequirement>SFT-DCMS-SINGLE</LicenseRequirement>
</Information>
<StringValue><![CDATA[]]></StringValue>
<!--file path to load file-->
</Setting>
```

## E.6 License Requirement

SAA 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.

	SAA
Managed System With SFT-DCMS-SINGLE	Take effect
Managed System Without SFT-DCMS-SINGLE	Not take effect Output SFT-DCMS-SINGLE license required message

Use SAA 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 the Node Product Keys.

---

## 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>
 <!--SuperServer Automation Assistant 1.0.0 (2023/09/23)-->
 <!--File generated at 2023-09-23_13:22:10-->
 <!--Usage notes:-->
 <!--You can remove unnecessary elements so that-->
 <!--their values will not be changed after update-->
 <!--Please refer to SAA User's guide 'Format of the BMC Configuration Text File' for more details.-->
 <?BMC CONFIG SOURCE BMC configuration for OOB usage?>
 <StdCfg Action="Change">
 <!--Supported Action:None/Change-->
 <!--Standard BMC configuration tables-->
 <FRU Action="None">
 <!--Supported Action:None/Change-->
 <Configuration>
 <!--Configuration for FRU data-->
```

- 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>
 <!--SuperServer Automation Assistant 1.0.0 (2023/09/23)-->
 <!--File generated at 2023-09-23_13:22:10-->
 <!--Usage notes:-->
 <!--You can remove unnecessary elements so that-->
 <!--their values will not be changed after update-->
 <!--Please refer to SAA User's guide 'Format of the BMC Configuration Text File' for more details.-->
 <?BMC CONFIG SOURCE BMC configuration for OOB usage?>
 <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 SAA, 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. SAA 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, SAA 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, SAA 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 SAA will export error messages. Similarly, for **<Setting>**, the attributes “**name**,” “**order**” (if applicable) and “**type**” should not be changed or removed. SAA 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 SAA 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: ea0413152cdeld98ebdca3fe6f0230904c9ef717
332909815: --alswrv 0 0 asymmetric: Red Hat Inc.: 1ff96dd8d1b2327228c04b03a772dbb2d8b79b1f
406705284: --alswrv 0 0 asymmetric: CentOS Secure Boot (key 1): f037c6eae36d4057a526c0ec6d5a95b324ee129
287390309: --alswrv 0 0 asymmetric: Microsoft Windows Production PCA 2011: a92902398e16c49778cd90f99e4f9ae17c55af53
983629943: --alswrv 0 0 asymmetric: Microsoft Corporation UEFI CA 2011: 13adbf4309bd82709c8cd54f316ed522988a1bd4
22744187: --alswrv 0 0 asymmetric: AddTrust External CA Root: adbd987a34b426f7fac42654ef03bde024cb541a
46692380: --alswrv 0 0 asymmetric: CentOS Linux kernel signing key: b70dcf0df2d9b7f29159248249fd6fe87b781427
384900254: --alswrv 0 0 asymmetric: CentOS Linux Driver update signing key: 7f421ee0ab69461574bb358861dbe77762a4201b
```

4. Configure the key information and follow the example below to create your own configuration file.

Example:

```
[req]
default_bits = 4096
distinguished_name = req_distinguished_name
prompt = no
string_mask = utf8only
x509_extensions = myexts
[req_distinguished_name]
O = <Your key name>
emailAddress = <Your Email>
[myexts]
basicConstraints=critical,CA:FALSE
keyUsage=digitalSignature
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid
```



**Note:**

To create a key pair, a configuration file is needed. You can copy and paste the example above to create and name a configuration file as "configuration\_file.config." Then modify the following variables in the configuration file.

- <Your key name>: the key name
  - <Your e-mail>: the e-mail address
-

---

5. Generate a public and private X.509 key pair.

Syntax:

```
[shell]# sudo openssl req -x509 -new -nodes -utf8 -sha256 -days <days> -batch \ -
config configuration_file.config -outform DER -out <public_key.der> -keyout \
<private_key.priv>
```



**Notes:**

- <days>: Valid certification days, e.g., 36500.
  - <public\_key.der>: The generated public key file, e.g., public\_driver\_key.der
  - <private\_key.priv>: The generated private key file, e.g., private\_driver\_key.priv
- 

Example:

```
[root@localhost Linux]# sudo openssl req -x509 -new -nodes -utf8 -sha256 -days 36500 -batch -config configuration_file.config -outform
DER -out public_key.der -keyout private_key.priv
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to 'private_key.priv'

```

6. Add your public key to the MOK list by using Linux mokutil.

Syntax:

```
[shell]# sudo mokutil --import public_key.der
```



**Notes:**

- You will be asked to enter and confirm a password for this MOK enrollment request.
  - public\_key.der: the generated public key file.
- 

Example:

```
[root@localhost Linux]# sudo mokutil --import public_key.der
input password:
input password again:
```

- 
7. Reboot the system and enroll the key.

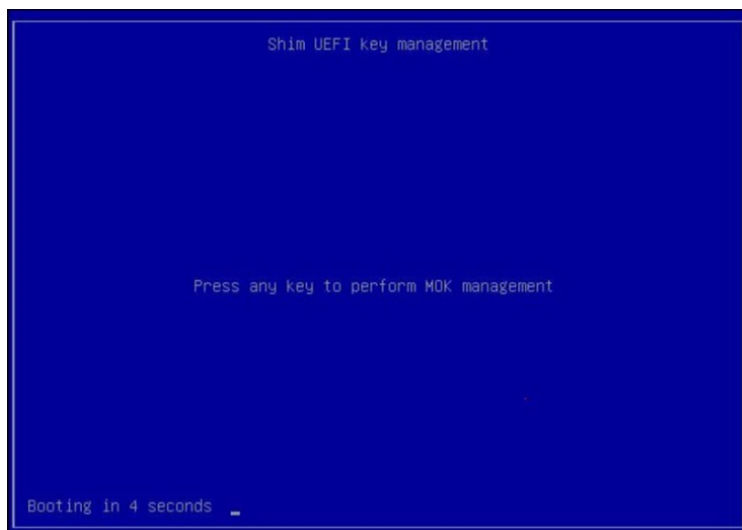


**Note:**

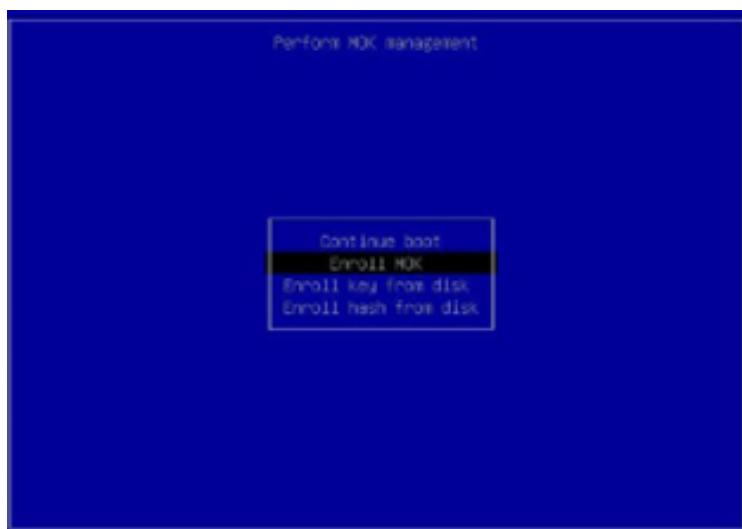
The MOK management main screen will appear immediately after reboot and last for 10 seconds. Please press any key as soon as you are under MOK management. If you miss this step, you will need to repeat step 6.

---

8. Press any key to continue.



9. Select **Enroll MOK**.



- 
0. Select **Continue** to enroll the key.



**Note:**

You can view your enrolled key by selecting View key 0.

---

1. Select **Yes**.
2. Input the password you set.
3. Select Reboot to reboot.
4. 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 X12/H12 and later platforms except H12 non-RoT systems

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.2 CMM

New password rules have been applied to CMM. You must follow these rules to create a CMM password.

- The password length is limited to 8 to 19 characters.
- All special characters are supported except for <space>.



---

The table lists all supported special characters.

!	\$	%	&	(	)	*	+
.	/	<	=	>	?	@	[
\	]	^	_	`	{		}
~	-	:	,	;	#		

## Appendix J. System Lockdown Mode Table

[ Group ] Command	Authority for System Lockdown Mode
	Read only
[ License Management ]	
ActivateProductKey	No
QueryProductKey	Yes
CpuOnDemand	No
[ Health Management ]	
CheckOOBSupport	Yes
CheckAssetInfo	Yes
CheckSystemUtilization	Yes
CheckSensorData	Yes
ServiceCalls	No
SystemPFA	No
MemoryHealthCheck	No
ChassisIntrusion	Yes
AlertManage	No
SuperDiag	Yes
SendDiagInterrupt	Yes
MonitorCDUStatus	No
TasManage	No
CheckSelfTest	No
HDTService	No
[ System Management ]	
GetFruInfo	Yes
RestoreFruInfo	No

ChangeFruInfo	No
GetSystemInfo	Yes
GetSystemCfg	Yes
ChangeSystemCfg	No
GetFanMode	Yes
SetFanMode	No
LocateServerUid	Yes
GetFirmwareInventoryInfo	Yes
ClearCMOS	No
<b>[ BIOS Management ]</b>	
UpdateBios (without --preserve_setting)	No
UpdateBios (with --preserve_setting)	No
GetBiosInfo	Yes
GetDefaultBiosCfg	Yes
GetCurrentBiosCfg	Yes
ChangeBiosCfg	No
LoadDefaultBiosCfg	No
SetBiosPassword	No
GetDmiInfo	Yes
EditDmiInfo	Yes
ChangeDmiInfo	No
ChangeDmiInfo	No
SetBiosPassword	No
EraseOAKey	No
GetBootOption	No
SetBootOption	No
SetHttpBoot	No
<b>[ BMC Management ]</b>	

UpdateBmc	No
GetBmcInfo	Yes
GetBmcCfg	Yes
ChangeBmcCfg	No
SetBmcPassword	No
GetKcsPriv	Yes
SetKcsPriv	No
LoadDefaultBmcCfg	No
TimedBmcReset	No
GetBmcUserList	Yes
SetBmcUserList	No
RmcpManage	Yes
GetSessionInfo	Yes
BmcWatchDog	No
SNMPManage	No
<b>[ System Event Log ]</b>	
GetEventLog	Yes
ClearEventLog	No
GetMaintenEventLog	Yes
ClearMaintenEventLog	No
GetHostDump	No
<b>[ CMM Management ]</b>	
UpdateCmm	No
GetCmmInfo	Yes
GetCmmCfg	Yes
ChangeCmmCfg	No
SetCmmPassword	No
LoadDefaultCmmCfg	No

GetBbpInfo	Yes
UpdateBbp	No
GetBladePowerStatus	Yes
SetBladePowerAction	No
BladePsuManage	Yes
BladeSummary	Yes
GetBmcUserList	Yes
SetBmcUserList	No
UpdateDummySwitch	No
<b>[ Storage Management ]</b>	
GetRaidControllerInfo	Yes
UpdateRaidController	No
GetRaidCfg	Yes
ChangeRaidCfg	No
GetSataInfo	Yes
GetNvmeInfo	Yes
GetPMemInfo	Yes
UpdatePMem	No
GetVROCCfg	Yes
ChangeVROCCfg	Yes
ControlNVMe	Yes
GetSmartData	Yes
GetSasExpanderInfo	Yes
UpdateSasExpander	No
<b>[ Power Management ]</b>	
GetPsuInfo	Yes
UpdatePsu	No
GetPowerStatus	Yes

SetPowerAction	Yes
DcmiManage	Yes
PowerPolicy	No
GetAcpiPowerStatus	Yes
GetPsFruInfo	Yes
<b>[ PCIeSwitch Management ]</b>	
GetPCleSwitchInfo	Yes
UpdatePCleSwitch	No
<b>[ Applications ]</b>	
RawCommand	Yes
GetUsbAccessMode	Yes
SetUsbAccessMode	No
KmsManage	No
RedfishApi	Yes
RemoteExec	No
RemoteConsole	No
RemoteScreenshot	No
RemoteKeyboard	No
Sol	No
FindBmcDevices	Yes
Shell	Yes
Prompt	Yes
<b>[ GPU Management ]</b>	
GetGpuInfo	Yes
UpdateGpu	No
DiagGpuStatus	Yes
GetGpuLog	No
<b>[ CPLD Management ]</b>	

GetCpldInfo	Yes
UpdateCpld	No
GetSwitchboardCpldInfo	Yes
UpdateSwitchboardCpld	No
GetBackplaneCpldInfo	Yes
UpdateBackplaneCpld	No
GetFanboardCpldInfo	Yes
UpdateFanboardCpld	No
GetAipCpldInfo	No
UpdateAipCpld	No
GetAomboardCpldInfo	Yes
UpdateAomboardCpld	No
GetMiscCpldInfo	Yes
UpdateMiscCpld	No
GetMidplaneSbbCpldInfo	Yes
UpdateMidplaneSbbCpld	No
GetNICCpldInfo	Yes
UpdateNICCpld	No
GetTransitionboardCpldInfo	Yes
UpdateTransitionboardCpld	No
<b>[ NIC Management ]</b>	
GetAocNICInfo	Yes
UpdatetAocNIC	No
<b>[ Multi-Node Management ]</b>	
GetTpInfo	Yes
ChangeTpInfo	No
GetMultinodeEcInfo	Yes
UpdateMultinodeEc	No

<b>[ VM Management ]</b>	
MountIsoImage	No
UnmountIsoImage	No
MountFloppyImage	No
UnmountFloppyImage	No
GetVmInfo	Yes
VmManage	No
VMShell	No
<b>[ NM Management ]</b>	
NmMeManage	No
GeneralNmManage	No
NmCpuManage	No
NmCupsManage	No
BmcNmManage	Yes
<b>[ Security Management ]</b>	
BiosRotManage	No
BmcRotManage	Yes
CpldRotManage	Yes
SecureBootManage	Yes
GetLockdownMode	Yes
SetLockdownMode	Yes
Attestation	No
SecureEraseRaidHdd	No
SecureEraseDisk	No
TpmProvision	No
GetTpmInfo (Supermicro OTA)	Yes
GetTpmInfo (Intel OTA)	Yes
TpmManage (Supermicro OTA)	No



---

TpmManage (Intel OTA)	No
GetCpuERoTInfo	Yes
UpdateCPUERoT	No
CPUERoTManage	Yes
FpgaRotManage	Yes
GetGpuERoTInfo	Yes
GetSpdmInfo	Yes
CmmRotManage	Yes
<b>[ FPGA Management ]</b>	
GetMotherboardFpgaInfo	Yes
UpdateMotherboardFpga	No
<b>[ MCU Management ]</b>	
GetMotherboardMcuInfo	Yes
UpdateMotherboardMcu	No

---

## Appendix K. Using SAA to Run 3rd -Party Tools

To run SAA with a third-party tool on remote systems, execute the RemoteExec command to connect to remote systems. For details on the RemoteExec command, see 5.11.8 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 SAA.

```
./saa -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 nvupdate64e && ./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 nvupdate64e” files make the files executable.
6. LLDP\_EN(.sh) is an update script from the vendor, nvupdate64e is the binary to update the firmware, and nvupdate.cfg is the configuration file required for nvupdate64e. The “./LLDP\_EN.sh” file will call nvupdate64e with nvupdate.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. SAA 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.

```
root@root:~/HGXA100/A100_v1.0_80G$ tree
```

```
.
├── chk_inband_firmware.sh
├── config
│ ├── passwd
│ └── version
│ └── 123456789_3CECEF1EDE4C
├── config_INB.txt
├── 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_INB.sh
└── startup.sh
```

7 directories. 22 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:

```
root@root:~/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 “SAA\_UpgradeGPU\_script.sh” or “SAA\_UpgradeGPU\_MMscript.sh” script and edit

---

“SAA\_Upgrade\_cfg.txt” under “SAA 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 “SAA\_UpgradeGPU\_script.sh” for upgrading single GPU system.

#Cmd1: Transfer and untar scripts/tools/firmware package

```
./saa -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

```
./saa -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

```
./saa -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 SAA command, UpdateGpuFw)

```
./saa -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 “SAA\_UpgradeGPU\_MMscript.sh” under “SAA 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
1 purpose=xyz.openbmc_project.Software.Version.VersionPurpose.Host
2 version=202205101037
3 ExtendedVersion=primary
4 MachineName=r12spd
5
```

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
```

```
1: MANIFEST
1 purpose=xyz.openbmc_project.Software.Version.VersionPurpose.Host
2 version=2.06
3 ExtendedVersion=scp-primary
4 MachineName=r12spd
```

2. Create a tar file including the firmware image and MAINFEST file:

```
$ tar -cvf r12spd_atf_xxxx.tar altr_scp_signed_x.xx.xxxxx.slim MANIFEST
```

## Appendix M. Component firmware information and update support matrix

Component	Component		
	Get Information	Update Firmware	RoT Management
BIOS	GetBiosInfo	UpdateBios	BiosRotManage
BMC	GetBmcInfo	UpdateBmc	BmcRotManage
CPLD	GetCpldInfo	UpdateCpld	CpldRotManage
CMM	GetCmmInfo	UpdateCmm	CmmRotManage
BBP	GetBbpInfo	UpdateBbp	N/A
PSU	GetPsuInfo	UpdatePsu	N/A
RAID Controller	GetRaidControllerInfo	UpdateRaidController	N/A
GPU	GetGpuInfo	UpdateGpu	N/A
PMem	GetPMemInfo	UpdatePMem	N/A
AOC NIC	GetAocNICInfo	UpdateAocNIC	N/A
AIP CPLD	GetAipCpldInfo	UpdateAipCpld	N/A
Switch	GetBladeSwitchInfo	UpdateBladeSwitch	N/A
SCP	GetScpInfo	UpdateScp	N/A
Multinode EC	GetMultinodeEcInfo	UpdateMultinodeEc	N/A
Backplane storage CPLD	GetBackplaneCpldInfo	UpdateBackplaneCpld	N/A
PCIe Switch	GetPCleSwitchInfo	UpdatePCleSwitch	N/A



---

PCIe Switch board CPLD	GetSwitchboardCpldInfo	UpdateSwitchboardCpld	N/A
Fan board CPLD	GetFanboardCpldInfo	UpdateFanboardCpld	N/A
AOM board CPLD	GetAomboardCpldInfo	UpdateAomboardCpld	N/A
Midplane SBB CPLD	GetMidplaneSbbCpldInfo	UpdateMidplaneSbbCpld	N/A
Motherboard FPGA	GetMotherboardFpgaInfo	UpdateMotherboardFpga	FpgaRotManage
Motherboard MCU	GetMotherboardMcuInfo	UpdateMotherboardMcu	N/A
SAS Expander	GetSasExpanderInfo	UpdateSasExpander	N/A
NIC CPLD	GetNICCpld	UpdateNICCpld	N/A
Dummy Switch	GetCmmInfo	UpdateDummySwitch	N/A
Transitionboard CPLD	GetTransitionboardCpldInfo	UpdateTransitionboardCpld	N/A

---

## Appendix N. GetGpuInfo/UpdateGpu supported platform matrix

Here is the table of GPU platforms mapping with Supermicro product SKUs and GetGpuInfo and UpdateGpu supporting status. GetGpuInfo command checks the detailed of GPU information and UpdateGpu command can update the firmware of GPU components.

Platform	Supermicro product SKUs	GetGpuInfo	UpdateGpu
Intel PVC	SYS-821GV-TNR	V	V
Intel Gaudi 2	SYS-820GH-TNR2	V	V
Intel Gaudi 3	SYS-822GA-NGR3	V	V
Nvidia H100/H200 Delta Next	<ul style="list-style-type: none"><li>SYS-821GE-TNHR</li><li>AS-8125GS-TNHR</li></ul>	V	V
Nvidia A100 Delta	<ul style="list-style-type: none"><li>SYS-420GP-TNAR</li><li>AS-4124GO-NART</li></ul>	V	V
Nvidia A100 Redstone	<ul style="list-style-type: none"><li>SYS-421GU-TNXR</li><li>SYS-420GU-TNXR</li><li>SYS-220GQ-TNAR</li><li>AS-2124GQ-NART</li></ul>	V	X (See Note)
AMD MI300X	<ul style="list-style-type: none"><li>AS-8125GS-TNMR2</li><li>SYS-821GE-TNMR2</li></ul>	V	V

Nvidia MGX	<ul style="list-style-type: none"> <li>ARS-111GL-NHR</li> </ul>	V	V
------------	-----------------------------------------------------------------	---	---



**Note:**

Due to BMC limitation, SAA does not support A100 Redstone now.

And here is the table of GPU platforms function commands mapping with Inband or OOB/Inband-RHI supporting matrix.

Platform	Command mode	GetGpuInfo	UpdateGpu
Intel PVC	In-Band	V (For PVC_IFWI and PVC_PSCBIN only)	V (For PVC_IFWI and PVC_PSCBIN only)
	OOB/Inband RHI	V (For PVC_UBB_CPLD, PVC_RETIMER, and PVC_AMC only)	V (For PVC_UBB_CPLD, PVC_RETIMER, and PVC_AMC only)
Intel Gaudi 2	In-Band	V (For GAUDI_SPI and gaudisecurity enable (security enable is only for production version))	V (For GAUDI_SPI, GAUDI_OAM_CPLD and GAUDI_UBB_CPLD only)
	OOB/Inband RHI	V (For GAUDI_RETIMER only)	V (For GAUDI_RETIMER only)
Intel Gaudi 3	In-Band	V	V (For GAUDI_SPI, GAUDI_OAM_CPLD only)
	OOB/Inband RHI	V	V (For GAUDI_RETIMER, GAUDI_UBB_CPLD only)
Nvidia A100 Delta	In-Band	X	X
	OOB/Inband RHI	V	V
Nvidia A100 Redstone	In-Band	X	X
	OOB/Inband RHI	V	X

---

Nvidia H100 Delta-Next	In-Band	X	X
	OOB/Inband RHI	V	V
AMD MI300X	In-Band	X	X
	OOB/Inband RHI	V	V
Nvidia MGX	In-Band	X	X
	OOB/Inband RHI	V	V

---

## Contacting Supermicro

### Headquarters:

Address: Super Micro Computer, Inc.  
980 Rock Ave.  
San Jose, CA 95131 U.S.A.  
San Jose, CA 95131 U.S.A.

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: [marketing@supermicro.com](mailto:marketing@supermicro.com) (General Information)  
[support@supermicro.com](mailto:support@supermicro.com) (Technical Support)

Website: [www.supermicro.com](http://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](mailto:sales@supermicro.nl) (General Information)  
[support@supermicro.nl](mailto:support@supermicro.nl) (Technical Support)  
[rma@supermicro.nl](mailto:rma@supermicro.nl) (Customer Support)

Website: [www.supermicro.nl](http://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](mailto:support@supermicro.com.tw)

---

Website: [www.supermicro.tw](http://www.supermicro.tw)