

SuperServer Automation Assistant

(SAA)

User's Guide

Revision 1.4.0

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
    - 1.2.6 Remote In-Band Usage Requirements (Remote Management Server)
    - 1.2.7 Remote In-Band Usage Requirements (Network)
    - 1.2.8 Remote In-Band Usage Requirements (Managed Systems)
  - 1.3 Typographical Convertions
- 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
  - 2.5 Setting Up VROC
- 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
  - 4.3.3.3. Auto-Activating Redfish Host Interface
  - 4.3.3.4. Pure Redfish Mode IPMI Raw Command Exception List
  - 4.3.3.5 Manually Activating Redfish Host Interface
- 4.3.4. Remote In-Band
  - 4.3.4.1 Remote In-Band Options
  - 4.3.4.2. Customizing Remote SAA Configurations
  - 4.3.4.3. Using Remote In-Band Mode
  - 4.3.4.4. Console Output
  - 4.3.4.5. 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
  - 4.4.2. System List Format for Specific Commands
    - 4.4.2.1. ActivateProductKey Command
    - 4.4.2.2. SetBiosPassword Command
    - 4.4.2.3. BIOS Configuration Related Commands
    - 4.4.2.4. SetBmcPassword Command
    - 4.4.2.5. BmcHostName Command
    - 4.4.2.6. BootStrappingAccount Command
    - 4.4.2.7. CpuOnDemand Command
- 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. PCIe-Switch Management
- 4.5.19. Security Management
- 4.5.20. MCU Management
- 4.5.21. Switch Management
- 4.5.22. Liquid Cooling 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
    - 4.10. JSON View
        - Supported Commands
        - Examples
        - Multi OOB Example
        - Schema
        - Field Descriptions
- 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. Managing TAS Functionality
    - 5.2.13. Checking and Reporting Basic Health Status of the BMC
    - 5.2.14. 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
    - 5.5.3.2 Downloading a BMC Configuration File
  - 5.5.4. Updating BMC Settings
  - 5.5.4.1 Uploading a BMC Configuration File
  - 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
  - 5.5.9.1. Loading Factory BMC Settings for NVIDIA Platform
  - 5.5.10. BMC Reset
  - 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. Managing the BMC Sessions
    - 5.5.18.1. Getting the BMC RMCP Session Information
    - 5.5.18.2. Managing the BMC Redfish Sessions
  - 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 Enabling Simple Network Management Protocol Trap Acknowledgement
  - 5.5.21.3 Disabling Simple Network Management Protocol Trap Acknowledgement
  - 5.5.21.4 Getting BMC Simple Network Management Protocol Community String
  - 5.5.21.5 Setting BMC Simple Network Management Protocol Community String
- 5.5.22 Managing a BMC IPV6 Static Route

- 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
  - 5.6.6. Setting SEL Time Mode
- 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. Blade Power Supply Unit Management
    - 5.7.12.1. Getting Blade Power Supply Unit Information
    - 5.7.12.2. Getting Blade Power Supply Unit Consumption
    - 5.7.12.3. Getting Blade System Fan Speed
    - 5.7.12.4. Setting Blade System Fan Speed

- 5.7.12.5. Getting Blade System Fan Mode
- 5.7.12.6. Setting Blade System Fan Mode
- 5.7.13 Profile Management
  - 5.7.13.1 Profile Update Rule
  - 5.7.13.2. Profile Management
  - 5.7.13.3. Updating CMM Configurations
  - 5.7.13.4. Updating Blade System Configurations
- 5.7.14 Getting Blade Summary
- 5.7.15 Getting the CMM User List
- 5.7.16 Setting the CMM User List
- 5.7.17 Updating Dummy Switch Firmware Image
- 5.7.18 Launching Blade Console
- 5.7.19 Managing Nodes within the Blade System
  - 5.7.19.1 Getting Blade Node Sensor
  - 5.7.19.2 Getting Blade Node Status
  - 5.7.19.3 Getting Blade Node Power
  - 5.7.19.4 Setting Blade Node Power
  - 5.7.19.5 Getting Blade Node IP Address
  - 5.7.19.6 Setting Blade Node IP Address
  - 5.7.19.7 Getting Blade Node DHCP
  - 5.7.19.8 Setting Blade Node DHCP
  - 5.7.19.9 Getting Blade Node MAC Address
  - 5.7.19.10 Setting Blade Node MAC Address
  - 5.7.19.11 Getting Blade Node Subnet Mask
  - 5.7.19.12 Setting Blade Node Mask
  - 5.7.19.13 Getting Blade Node Gateway
  - 5.7.19.14 Setting Blade Node Gateway
  - 5.7.19.15 Getting Blade Node Name
  - 5.7.19.16 Setting Blade Node Name
  - 5.7.19.17 Getting Blade Node UID
  - 5.7.19.18 Setting Blade Node UID
  - 5.7.19.19 Getting Blade Node System Model
- 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
  - 5.9.11. Getting and Setting CPU Power Limit of the managed system
  - 5.9.12. Getting PowerShelf Information
  - 5.9.13. Updating Power Unit Firmware in the PowerShelf
- 5.10. PCIe-Switch Management
  - 5.10.1. Getting PCIeSwitch 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
- 5.11.18. Remote Screenvideo

- 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
  - 5.12.5. Getting and Setting GPU Power Limit of the managed system
- 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
  - 5.15.5. Getting Multi-Node LCMC Firmware Image Information
  - 5.15.6. Updating the Multi-node LCMC 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
  - 5.16.8. Managing a BMC Host 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
    - 5.18.18 GB200 Certificate Management
        - 5.18.18.1. Performing Various Certificate Management Actions
        - 5.18.18.2. Certificate Management Use Cases
- Generating a private key:
- Generating a Certificate:
- Creating the PEM File:
- 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
- 5.21 Switch Management
    - 5.21.1 Nvidia Switch Management

        - 5.21.1.1 Performing Various Nv Switch Management Actions
        - 5.21.1.2 Nv Switch Management Use Cases
      - 5.21.2 Receiving the Switch Firmware Image Information
      - 5.21.3 Updating the Switch Firmware
      - 5.21.4 Rebooting the Switch
    - 5.22 Liquid Cooling Management
      - 5.22.1. Monitoring CDU Status
        - 5.22.1.1. Getting CDU Information
        - 5.22.1.2. Setting CDU Alert Setting
        - 5.22.1.3. CDU Alert Settings JSON File Format
      - 5.22.2. Updating the CDU 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.1.1 X12/H12 and later platforms except H12 non-RoT systems
  - I.1.2 Ampere OpenBMC platforms
  - 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
- Appendix O. Power Capping
  - O.1 Introduction
  - O.2 Power Capping Methods
  - O.3 Scenario Example
    - O.3.1 Scenario Example for PowerPolicy Command
    - O.3.2 Scenario Example for DcmiManage Command
    - O.3.3 Scenario Example for ChangeBmcCfg Command
  - O.4 Summary
- Appendix P. How to Mount an ISO Image and Set It as a Boot Option
  - P.1 Introduction
  - P.2 Example
- Appendix Q. Sample Configuration Tables for BMC and CMM
    - Q.1 Sample Configuration Tables
      - Q.1.1 Sample BMC Configuration Table
      - Q.1.2 Sample CMM Configuration Table
      - Q.1.3 NVIDIA BMC Configuration Tables (Examples)
- Appendix R. AD/LDAP Account Login on BMC
  - R.1 Configuring AD/LDAP Account Login Settings
    - R.1.1 Configuring AD/LDAP Account Login Settings through BMC Web Interface
    - R.1.2 Configuring AD/LDAP Account Login Settings through SAA Commands
  - R.2 Using AD/LDAP Account Login
- 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 1.4.0

Release Date: October 9, 2025

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 © 2025 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	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. Added the options --usb and --action List for the SuperDiag command. 13. Supported MGX_GPU, MI300X, and ONBOARD_RETIMER items in the UpdateGPU command.
Dec-27-2024	1.2.0	1. Added the SetSELTimeMode command to support setting SEL time. 2. Added support for the --file option in the CheckAssetInfo command. 3. Added the BmcIPv6StaticRouteManage command. 4. Added the Ch command. 5. Added the GpuPowerManage command.
May-14-2025	1.3.0	1. Added the LocateServerUid command to support in-band Redfish. 2. Added the BmcReset command to replace the TimedBmcReset command. 3. Added the GetPostCodeLog and ClearPostCodeLog commands. 4. Added Redfish support for the LoadDefaultBiosCfg command. 5. Added Redfish support for the GetNVMeInfo command. 6. Added support for the GAUDI_UBB_CPLD2 item to the UpdateGpu command.

		7. Added support for the CpuPowerManage command. 8. Added Redfish support to the CheckSensorData command.
Oct-9-2025	1.4.0	1. Added support for the GetPowerShelfInfo command. 2. Added support for the UpdatePowerShelf command. 3. Added support for the UpdateCDU 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.
- 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 Boot Option Information.
- Sets Boot Option 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.
- Controls the BMC Redfish 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.
- Manages BMC IPv6 static route.

- 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.
  - Sets the managed system SEL time.
- 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.
  - 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.
  - Gets/Sets the CPU Power limit value of the managed system.
  - Displays information about power units in the managed Power Shelf system.
  - Update power unit firmware in the managed Power Shelf 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.
  - Enters SAA shell mode.
  - Manages the BMC connection configuration in SAA shell mode.
  - Enables remote operation and monitoring for system diagnostics
- 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.
  - Gets/Sets the GPU power limit value 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.
  - Gets the multi-node LCMC information of the managed system.
  - Updates the multi-node LCMC.
- 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.
- Switch Management
    - Gets the switch information of the managed system/input switch image file.
    - Updates switch firmware.
    - Reboots the Switch.
- Liquid Cooling Management

- Monitors the CDU system to get status and set settings remotely.
- Updates the CDU information of the managed system.

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 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	BIOS Version 1.0 or later for X12/H12 select systems BIOS Version 1.0d or later for Ampere® Altra®/Altra® Max processor family on R12 platforms
Operating System	Linux: Red Hat Enterprise Linux 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: From Windows Server 2008 R2 SP1 (x64) to Windows Server 2019 FreeBSD: FreeBSD 12 (x86_64) or later ESXi: ESXi 8.0



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*.

Protocol and Port Requirements

Command	Network Requirements
In-Band commands through BIOS SMI or IPMI KCS.	No external protocol is required.
In-Band commands through Redfish Host Interface.	HTTPS protocol through 169.254.3.254 using TCP with port 443.

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
ESXi	ESXi-phymem-driver	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

1.2.6 Remote In-Band Usage Requirements (Remote Management Server)

To run Remote In-Band 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 Systems	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 8.0

1.2.7 Remote In-Band Usage Requirements (Network)

To run Remote In-Band commands, the following network communication protocols and ports are required:

Command	Network Requirements
All Remote In-Band commands	SSH protocol through IPv4 TCP with port 22. SFTP protocol through IPv4 TCP with port 22.

1.2.8 Remote In-Band Usage Requirements (Managed Systems)

With the use of Remote In-Band, SAA can perform BIOS/BMC Management functions for selected Supermicro motherboards/systems. The managed system must meet the requirements outlined in *1.2.4 In-Band Usage Requirements* and *1.2.5 Additional In-Band Usage Requirements*.

1.3 Typographical Convertions

This manual uses the following typographical conventions.

Convention	Definition
Bold	Keywords needing attention are in bold.
Italics	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-saa-uw_x.x.x-0.x00.000x_xxxxxxxx.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-saa-uw_x.x.x-
0.x00.000x_xxxxxxxx.zip
```

   After installing the component, please reboot the system.

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 SMC-ESXi-phymem-driver_x.x.x-0.x00.000x_xxxxxxxx-package.zip
root@10.10.10.10:/vmfs/volumes/datastore1
```

4. Set .saarc ESXi_driver veriable like below:
   ESXi_driver = /vmfs/volumes/datastore1/SMC-ESXi-phymem-driver_x.x.x-0.x00.000x_xxxxxxxx-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 step 1, 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.



Note:
If the unsigned version of SAA is used, please add the "--no-sig-check" when installing the component, so the installing command would be:

```
esxcli software component apply -d /tmp/SMC-ESXi-saa-
uw_x.x.x-0.x00.000x_xxxxxxxx.zip --no-sig-check
```

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 below commands:

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

   to the /etc/rc.local.d/local.sh file in ESXi system.

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

# local configuration options

# Note: modify at your own risk!  If you do/use anything in this
# script that is not part of a stable API (relying on files to be in
# specific places, specific tools, specific output, etc) there is a
# possibility you will end up with a broken system after patching or
# upgrading.  Changes are not supported unless under direction of
# VMware support.

# Note: This script will not be run when UEFI secure boot is enabled.
cp /opt/supermicro/bin/custom_service.xml /etc/vmware/firewall/
esxcli network firewall refresh
sh /opt/supermicro/bin/network.sh
exit 0
```

2. Reboot the system.

custom_service.xml:

```
<!-- Firewall configuration information -->
<ConfigRoot>
 <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>
</ConfigRoot>
```

whcih is required for ESXi system to add the ports to whitelist.



Notes:

- The /vmfs/volumes/datastoreX folder might be different in ESXi system. Please check it in your ESXi system first.
- 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.

2.5 Setting Up VROC

Intel® Virtual RAID on CPU (Intel® VROC) is a hybrid RAID solution that connects NVMe SSDs directly to the PCIe lanes of Intel® Xeon® processors, eliminating the need for a RAID host bus adapter (HBA) and improving system performance. To use VROC with SAA, follow these steps:

1. **Install VROC Key**

   Intel® VROC requires a VROC key to be installed on the motherboard . The features supported depend on the type of key used.

2. **Install VROC Driver**

   The VROC Redfish API requires the VROC driver to be installed. To use VROC with SAA, the VROC driver must be installed.

For more details, please refer to *Supermicro's official page* and *Intel's official page*.



Note: To use VROC with SAA, you must enter the operating system and wait for a period of time until VROC is fully initialized.

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-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":"11111111111111111112222222222222223333333333333abababababababababababbabcdcdcdcdcdcdcdccdcdcddcdefefefefefefefefefeefefefefghghghghghghghghghghgh"}}

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.
-I	<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.
--json_view	Outputs results in JSON format for supported commands only.
--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 system management only)
--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
tcp_timeout	[1]240	Sets the timeout for checking TCP 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 .saarc file only

		the file name contains an IPv6 address.	
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/Supermicro-vmware-sum-driver_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 default value is 1000 Mbps.	the .saarc file only
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
oob_reboot_delay_time	[1]0	Sets the out-of-band reboot delay time in seconds.	the .saarc file only
redfish_only	[1]on	Sets the pure redfish flag by default, the default value is off.	the .saarc file only
command usage log	[1]enable	Enables the saa.log file by default, the default value is enable.	the .saarc file only
retry_count	[1]1	Sets the number of retry workflow[8] attempts, a number	the .saarc file only

		from 0 to 5, set 0 to disable.	
debug_redfish	[1]0	Sets the redfish debug level[9] value from 0 to 3.	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.

[8]Currently supported command: UpdateBmc.

[9]Prints Redfish API request and response to output, it is recommended to redirect outputs into a file when using this debug flag. Debug levels: 1=url; 2=url, payload, response_body; 3=url, payload, response_body, response_header

The .saarc configuration file can be specified in three ways, listed in order of priority:

1. **Command option** (highest priority): Use --rc_path to specify the .saarc file path
2. **SAA directory** (intermediate priority): Place the .saarc file in the same directory as the SAA executable
3. **User home directory** (lowest priority): Place the .saarc file in the user's home directory

A sample configuration file saarc.sample is included with the SAA release package. You can rename saarc.sample to .saarc and place it in your preferred location based on the priority order above. The system will automatically use the highest priority .saarc file found

An example configuration is provided below.



Notes:

- In Linux/FreeBSD, when using sudo, the effective user becomes root, and thus the home directory is /root.
- In Windows, copy the SAA configuration file and rename it to .saarc using Command Prompt.
- In ESXi, there is no user home directory, so `/vmfs/volumes/datastore1` is used as a replacement.

```
# 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

# set out of band reboot delay time in seconds.
#oob_reboot_delay_time = 0

# set the pure redfish flag by default, the default value is off.
#redfish_only = on

# set command usage log enable/disable
#command_usage_log = enable

# set the number of retry workflow attempts, a number from 0 to 5, set 0 to
disable.
#retry_count = 1

# set the redfish debug level value from 0 to 3.
# 1.display url   2.display url,payload,response_body   3.display
url,payload,response_body,response_header
#debug_redfish = 0
```

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.

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
```

4.3.3.3. Auto-Activating Redfish Host Interface

On Intel X14 systems, the Redfish Host Interface (RHI) must be disabled by default to achieve the lowest power consumption with Package C-state PC6 enabled. For SuperServer Automation Assistant (SAA) commands required to use RHI, RHI must be activated first. To simplify the process, SAA can automatically activate RHI before running SAA commands. Then SAA will deactivate RHI if it is activated by SAA, immediately after the SAA command is completed.

SAA will do the following actions to activate/deactivate RHI automatically.

```
1. Check the RHI status. If the RHI status is deactivated, activate RHI.
2. If the RHI connection is not available, execute the OS specific
script(s)/shell command to enable RHI.
   2.a Linux: Linux_enable_RHI.sh
   2.a-1 SUSE: Linux_enable_RHI.sh, SuSE12_Firewall_WhiteList.sh
   2.b Windows: No action needed
   2.c FreeBSD: FreeBSD_setup_RHI.sh
   2.d ESXi: esxcli network
3. If the RHI connection is available, proceed the SAA command flow directly.
4. If the RHI connection is not available, stop the process, please contact
Supermicro for further support.
5. At the end of SAA command execution, deactivate RHI, if RHI is activated in
Step 1.
6. If the running OS is SUSE, Clear_SuSE12_Firewall_disable_RHI.sh will be
```

```
executed to remove RHI from firewall whitelist.
```

4.3.3.4. Pure Redfish Mode IPMI Raw Command Exception List

In in-band pure Redfish mode, some IPMI raw commands are still required to make the necessary RHI connection. Please contact Supermicro for more details

4.3.3.5 Manually Activating Redfish Host Interface

For SuperServer Automation Assistant (SAA) commands that require RHI, RHI must first be activated. On GB200 systems, Redfish Host Interface (RHI) is not configured due to specific system constraints or configurations. To configured RHI manually, fill in the required details, including the BMC host IP, username, and password, in the "GB200_enable_RHI.sh" script.

```
#!/bin/bash
# Scipt to temporarily enable Redfish Host Interface on GB200 system.
# Please fill in below variables
BMC=
USERNAME=""
PASSWORD=""
URL="https://$BMC/redfish/v1/Managers/BMC_0/EthernetInterfaces/hostusb0"
```

4.3.4. Remote In-Band

The Remote In-Band mode can be used to securely execute commands and transfer files between operating systems (OSs) over the network using the SSH protocol. SAA acts as an SSH client and connects to an SSH server on the remote system for remote management.
Remote In-Band supports two authentication methods:

1. **Password-Based Authentication**
   Authenticate using the OS username and password to log in to the remote system.

2. **Public Key Authentication**
   Authenticate using an SSH private key. If the private key is encrypted, the private key password is required.

To learn how to provide authentication from the command line, see 4.3.4.3 Using Remote In-Band Mode.



Notes:

- The remote managed system must have **OpenSSH** installed to allow SSH connections.
- For remote **FreeBSD** systems, the sudo command must also be installed by using "pkg install sudo".
- 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.

4.3.4.1 Remote In-Band Options

The available Remote In-Band options are listed in the following table.

Options	Description or usage
--oi	<OS IP address>
--ou	<OS user ID>
--op	<OS user password> (Password-Based Authentication)
--os_key	<OS private key> (Public Key Authentication)
--os_key_pw	<OS private key password> (Public Key Authentication)
--remote_saa	<sets remote SAA path>
--remote_saa_rc	<sets .saarc file path in the remote system>

4.3.4.2. 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 the path below on the remote system, and specify the remote_saa_path setting.

   Linux and FreeBSD:

   ~/supermicro/.remoteSaarc

   Windows:

   %HomePath%\supermicro\.remoteSaarc

   VMware ESXi:

   /vmfs/volumes/datastore1/.remoteSaarc

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	Sets the file transfer folder for remote SAA execution	.remoteSaarc file only

	Windows: %HomePath%\supermicro VMware ESXi: /vmfs/volumes/datastore1/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.

4.3.4.3. Using Remote In-Band Mode

To use the Remote In-Band mode, specify the command interface using the -I <InterfaceName> option. Two interfaces are available:

1. **-I Remote_INB**

This interface is used for standard Remote In-Band, allowing In-Band commands to be executed on the remote system.

Syntax:

Single System (Password-Based Authentication)	
Remote In-Band	./saa -I Remote_INB --oi <OS IP address> --ou <OS user ID> --op <OS user password> -c <command> [command options]

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 **Public Key Authentication** by specifying the OS private key using the **--os_key** option. If the private key is encrypted, specify the private key password with the **--os_key_pw** option. For the sake of simplicity, only the syntax for password-based authentication syntax for simplicity.

Single System (Public Key Authentication)	
Remote In-Band	./saa -I Remote_INB --oi <OS IP address> --ou <OS user ID> --os_key <OS private key> [--os_key_pw <OS private key password>] -c <command> [command options]

2. **-I Remote_RHI**

This interface is used for Remote In-Band through Redfish Host Interface, allowing In-Band commands to be executed on the remote system through the Redfish Host Interface.

When using this interface, BMC credentials (-u <username> and -p <password>) are required — unless the remote system supports either **AuthNone Authentication** or **Bootstrapping Account** (**see 4.3.3 Redfish Host Interface**), in which case the BMC credentials may be omitted.

Syntax:

Single System (Password-Based Authentication)	
Remote In-Band	./saa -I Remote_RHI [-u <username> -p <password>] --oi <OS IP address> --ou <OS user ID> --op <OS user password> -c <command> [command options]

Alternatively, you can use **Public Key Authentication** by specifying the OS private key using the **--os_key** option. If the private key is encrypted, provide the private key password with the **--os_key_pw** option. For clarity, only the syntax for password-based authentication is presented in the subsequent content.

Single System (Public Key Authentication)	
Remote In-Band	./saa -I Remote_RHI [-u <username> -p <password>] --oi <OS IP address> --ou <OS user ID> --os_key <OS private key> [--os_key_pw <OS private key password>] -c <command> [command options]



Note:
To set up Public Key Authentication, follow these steps:
1. Generate an SSH Key Pair: ssh-keygen -f <path_to_keys>

2. Transfer the Public Key to the remote system: ssh-copy-id -i <path_to_public_key> <username>@<hostname_or_IP>

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. 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 {-I Remote_INB | -I 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 (Password-Based Authentication):
        OS_IP_or_HostName OS_Username OS_Password
    Format 2 (Public Key Authentication):
        OS_IP_or_HostName OS_Username OS_PrivateKey
OS_Privatekey_Password(leave empty if no password)
```

Two formats are supported for Remote Redfish Host Interface (Remote_RHI) as follows.

```
    Format 1 (Password-Based Authentication):
        OS_IP_or_HostName OS_Username OS_Password BMC_Username
BMC_Password
    Format 2 (Public Key Authentication):
        OS_IP_or_HostName OS_Username OS_PrivateKey
OS_Privatekey_Password(leave empty if no 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 5.1.1 Activating the Node Product Keys.
- For the SetBiosPassword command, different formats are used. Refer to 5.4.11 Setting Up a BIOS Administrator Password.
- For the RemoteExec command, different formats are used. Refer to 5.11.8 Remote Execution.
- For the CpuOnDemand command, different formats are used. Refer to 5.1.3 Getting and activating CpuOnDemand Function for the action of 2.
- 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 2
```

```
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 2

```
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.
```

4.4.2. System List Format for Specific Commands

When managing multiple systems, certain commands require specific field data to properly interact with target systems.
The usage for multiple systems is listed below.

Multiple Systems

OOB	saa -l < **system list file** > [-u <username> -p <password>] -c <command> [command options]
Remote In-Band	saa {-l Remote_INB | -l Remote_RHI} -l < **system list file** > -c <command> [command options] [--remote_saa <remote SAA path>]

For multiple systems usage, managed systems should be enumerated row by row in the system list file. The system list file format is fixed for specific commands to ensure consistent data structure and reliable command execution across all target systems. The details for the system list file will be listed in the following chapters.

4.4.2.1. ActivateProductKey Command

- **Multiple Systems OOB usage**

Two formats are supported as follows:

```
Format 1: BMC_IP_or_HostName Node_Product_Key
Format 2: BMC_IP_or_HostName Username Password Node_Product_Key
```

For format 1, it is required to specify both “-u” and “-p” options in the command line. For format 2, the “-u” and “-p” options are optional in the command line. In this case, the Username/Password in the system list file overwrites the the “-u” and “-p” options in the command line.

- **Multiple Systems Remote In-Band usage**

Two formats are supported for multiple Remote In-Band as follows:

```
Format 1: OS_IP_or_HostName OS_Username OS_Password Node_Product_Key
Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey
OS_Privatekey_Password Node_Product_Key
```

Two formats are supported for multiple Remote Redfish Host Interface as follows:

```
Format 1: OS_IP_or_HostName OS_Username OS_Password BMC_Username
BMC_Password Node_Product_Key
Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey
```

```
OS_Privatekey_Password OS_Password BMC_Username BMC_Password
Node_Product_Key
```

Note that the Node_Product_Key field is **REQUIRED**. Since the node product key should be unique for the managed system, you should specify a Node_Product_Key corresponding to each system for Format 1 or Format 2 without using the "-key" option. If you provide the node product key with the "key_file" option in command line, the option value will overwrite the value in system list file.

4.4.2.2. SetBiosPassword Command

- **Multiple Systems OOB usage**

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, the “-u” and “-p” options are optional in the command line. In this case, the Username/Password in the system list file overwrites the the “-u” and “-p” options in the command line.

- **Multiple Systems Remote In-Band usage**

Two formats are supported for multiple Remote In-Band as follows:

```
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.

Note that the New_BIOS_Password and Current_BIOS_Password fields are both **REQUIRED**.
When executing the SetBiosPassword command through multi-node usage, the new

and current BIOS Administrator passwords should be assigned in the system list file without using command line options “--new_password”, “--pw_file”, “--current_password”, and “--cur_pw_file”.

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, you must still include an empty field (single space) to ensure correct field parsing.

4.4.2.3. BIOS Configuration Related Commands

When executing any of the following commands, ensure that you use the system list format described in this section:
GetCurrentBiosCfg, GetDefaultBiosCfg, ChangeBiosCfg, LoadDefaultBiosCfg, GetSystemCfg, ChangeSystemCfg, ClearEventLog, SetHttpBoot, KmsManage, UpdatePMem, SecureEraseDisk.

- **Multiple Systems OOB Usage**

Two formats are supported as follows:

```
Format 1: BMC_IP_or_HostName Current_BIOS_Password
Format 2: BMC_IP_or_HostName Username Password Current_BIOS_Password
```

For format 1, it is required to specify both “-u” and “-p” options in the command line.
For format 2, the “-u” and “-p” options are optional in the command line. In this case, the Username/Password in the system list file overwrites the “-u” and “-p” options in the command line.

- **Multiple Systems Remote In-Band usage**

Two formats are supported for multiple Remote In-Band as follows:

```
Format 1: OS_IP_or_HostName OS_Username OS_Password Current_BIOS_Password
Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey
OS_Privatekey_Password Current_BIOS_Password
```

Note that the Current_BIOS_Password field is **OPTIONAL**.
When executing the BIOS configuration related commands through multi-node usage, the current BIOS Administrator password should be assigned in the system list file the "--current_password" and "--cur_pw_file" command line options.

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, this field can be removed or filled with an empty value (single space).

If the command is executed under pure Redfish mode, the Current_BIOS_Password field is not needed and should be removed from the system list.

4.4.2.4. SetBmcPassword Command

- **Multiple Systems OOB usage**

Two formats are supported as follows:

```
Format 1: BMC_IP_or_HostName New_Password
Format 2: BMC_IP_or_HostName Username Password New_Password
```

For format 1, it is required to specify both "-u" and "-p" options in the command line.
For format 2, the "-u" and "-p" options are optional in the command line. In this case, the Username/Password in the system list file overwrites the "-u" and "-p" options in the command line.

- **Multiple Systems Remote In-Band usage**

Two formats are supported for multiple Remote In-Band as follows:

```
Format 1: OS_IP_or_HostName OS_Username OS_Password New_Password
Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey
OS_Privatekey_Password New_Password
```

Note that the New_Password field is **REQUIRED**.
When executing the SetBmcPassword command through multi-node usage, the new

BMC password should be assigned in the system list file without using the --new_password command line option.

4.4.2.5. BmcHostName Command

- **Multiple Systems OOB usage**

Two formats are supported as follows:

```
Format 1: BMC_IP_or_HostName New_BMC_HostName
Format 2: BMC_IP_or_HostName Username Password New_BMC_HostName
```

For format 1, it is required to specify both “-u” and “-p” options in the command line.
For format 2, the “-u” and “-p” options are optional in the command line. In this case, the Username/Password in the system list file overwrites the “-u” and “-p” options in the command line.

- **Multiple Systems Remote In-Band usage**

Two formats are supported for Multiple Remote In-Band as follows:

```
Format 1: OS_IP_or_HostName OS_Username OS_Password New_BMC_HostName
Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey
OS_Privatekey_Password New_BMC_HostName
```

Two formats are supported for Multiple Remote Redfish Host Interface as follows:

```
Format 1: OS_IP_or_HostName OS_Username OS_Password BMC_Username
BMC_Password New_BMC_HostName
Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey
OS_Privatekey_Password OS_Password BMC_Username BMC_Password
New_BMC_HostName
```

Note that the New_BMC_HostName field is **REQUIRED** when setting a new BMC hostname. For the "--action Get" option, this field is not needed and should be removed from the system list.
Since the BMC hostname should be unique for the managed system, you should specify a New_BMC_HostName corresponding to each system for Format 1 or Format 2 without using the "--hostname" option.

4.4.2.6. BootStrappingAccount Command

- **Multiple Systems Remote In-Band usage**

Two formats are supported for Multiple Remote Redfish Host Interface as follows:

```
Format 1: OS_IP_or_HostName OS_Username OS_Password BMC_Username
BMC_Password BootStrappingAccount_Username
Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey
OS_Privatekey_Password OS_Password BMC_Username BMC_Password
BootStrappingAccount_Username
```

Note that the BootStrappingAccount_Username field is **REQUIRED** when deleting a BootStrapping Account User. For options other than "--action DeleteAccount", this field is not needed and should be removed from the system list.
Since the BootStrapping Account User is unique for the managed system, you should specify a BootStrappingAccount_Username corresponding to each system for Format 1 or Format 2 without using the “--user_name” option.

4.4.2.7. CpuOnDemand Command

- **Multiple Systems OOB usage**

Two formats are supported as follows:

```
Format 1: BMC_IP_or_HostName PPIN
Format 2: BMC_IP_or_HostName Username Password PPIN
```

For format 1, it is required to specify both “-u” and “-p” options in the command line.
For format 2, the “-u” and “-p” options are optional in the command line. In this case, the Username/Password in the system list file overwrites tthe “-u” and “-p” options in the command line.

- **Multiple Systems Remote In-Band usage**

Two formats are supported for multiple Remote Redfish Host Interface as follows:

```
Format 1: OS_IP_or_HostName OS_Username OS_Password BMC_Username
BMC_Password PPIN
```

Format 2: OS_IP_or_HostName OS_Username OS_PrivateKey OS_Privatekey_Password OS_Password BMC_Username BMC_Password **PPIN**

Note that the PPIN field is **REQUIRED** with the "--action GetOnDemandState" option. Since the PPIN is unique for the CPU, you should specify a PPIN corresponding to each CPU for Format 1 or Format 2 without using option the “--hw_id” option.

4.5. Command Options

4.5.1. License Management

License Management	
Commands	**Long Options**
ActivateProductKey	**--key <node product key value> (Optional)** Uses the node product key to activate the managed system. **--key_file <node product key file> (Optional)** Uses the file of node product key to activate the managed system.
QueryProductKey	**--json_view (Optional)** Sets the output format to JSON. **--show_index (Optional)** Prints the key index information. **--showall (Optional)** Prints the key index and full key information.
CpuOnDemand	**--action <action>** Sets action to: 1 = GetHwInfo 2 = GetOnDemandState 3 = SetLicenseActivateCode 4 = EnablePPIN **--file <file name> (Optional)** Saves hardware information to file. **--overwrite (Optional)** Overwrites the hardware ID file.

	--cpu_id <CPU ID> (Optional) CPU ID to indicate CPU socket. **--cfg_file <Config file> (Optional)** IOD-agent config file **-v (Optional)** Prints extra info of CAP and registers. **--hw_id <Hardware ID> (Optional)** Hardware ID to indicate the PPIN of the CPU socket **--hw_id_file <Hardware ID file> (Optional)** Hardware ID file with the format of "BMC MAC;CPU ID;PPIN". **--squash (Optional)** Squashes the state reports into one file. **--plain_text (Optional)** Prints the on-demand state as plain text. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--skip_gap (Optional)** Skips the gap of LAC revision id and continue on provisioning. **--lac_file <LAC map file>** LAC+ file in the format of "PPIN;LAC+".

4.5.2. Health Management

Health Check	
Commands	**Long Options**
CheckOOBSupport	**--json_view (Optional)** Sets the output format to JSON.
CheckAssetInfo	**--json_view (Optional)** Sets the output format to JSON. **--file <file name> (Optional)** Saves the asset information to a file.

	Prints the asset information on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
CheckSensorData	**--json_view (Optional)** Sets the output format to JSON. **--sdr_id <SDR id> (Optional)** The SDR ID for delete. **--sdr_major_version <SDR major version> (Optional)** The SDR major version. **--sdr_minor_version <SDR minor version> (Optional)** The SDR minor version. **--redfish (Optional)** Enables pure Redfish support. **--showall (Optional)** Shows the sensor all threshold values of the managed system. **--action <action> (Optional)** Sets action to: 1 = Show 2 = Del 3 = GetVer 4 = SetVer **--temp_unit <TEMP_UNIT> (Optional)** Specifies the temperature unit to use. Acceptable values: 'C' for Celsius, 'F' for Fahrenheit.
CheckSystemUtilization	None
ServiceCalls	**--file <file name>** Monitors the host with the given XML-style file listing system event logs and sensor data records to be monitored.
SystemPFA	**--action <action>** Sets action to: 1 = GetCurrentStatus 2 = Enabled

	3 = Disabled **--json_view (Optional)** Sets the output format to JSON. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting.
MemoryHealthCheck	**--action <action>** Sets action to: 1 = GetCurrentStatus 2 = Persistent 3 = Enable 4 = Disable **--json_view (Optional)** Sets the output format to JSON. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting.
ChassisIntrusion	**--action <action>** Sets action to: 1 = Status 2 = Clear
AlertManage	**--action <action>** Sets action to: 1 = listMessage 2 = sendTest(only support OOB & Redfish_HI) **--message_type <List of message type>** Sets message type to: 1 = snmpv1 3 = snmpv3 4 = redfish **--after <datetime> (Optional)** Queries trap messages after specified time. **--before <datetime> (Optional)**

	Queries trap messages before specified time. **--ip <Sender IP> (Optional)** Queries trap message of the specified IP address. **--page <Page> (Optional)** Sets Page number and the default value is first page. **--limit <limit> (Optional)** Sets quantity of data with one page,and range is 10 to 100 The default value is twenty.
SuperDiag	**--action <action>** Sets SuperDiag action to: 1 = Start 2 = Download 3 = Display 4 = List **--file <file name> (Optional)** Start action: Mounts the ISO image to run diagnostics. Download/Display action: Enters the filename for diagnostic results. **--overwrite (Optional)** Overwrites the diagnostic results file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--image_url <URL> (Optional)** The URLs to access the shared image file. SAMBA URL: 'smb://<hostname or IP>/<shared point>/<file path>' SAMBA UNC: '\<hostname or IP><shared point><file path>' HTTP URL: 'http://<hostname or IP>/<shared point>/<file path>' HTTPS URL: 'https://<hostname or IP>/<shared point>/<file path>' **--dev_id <Device ID> (Optional)** The specified device to mount ISO image. The supported device ID: [1-3] **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--type <type> (Optional)** Sets display type to: 1 = Info 2 = Pass 3 = Fail **--index <index> (Optional)**

	The specified index to mount local USB. **--line <line> (Optional)** Prints the number of lines at a time. **--keyword <keyword> (Optional)** Prints results that match the keyword. **--embedded (Optional)** For action Start: Starts a diagnostic in embedded mode. For action Download: Downloads the diagnostic report for embedded SDO. **--usb (Optional)** For action Start: Starts a diagnostic with local USB device. For action List: Lists available device indexes to mount local USB.
SendDiagInterrupt	None
TasManage	**--action <action>** Sets action to: GetInfo Pause Resume Refresh Clear SetPeriod **--period <Period> (Optional)** Sets the TAS update period in seconds (between 5 and 60).
CheckSelfTest	None
HDTService	**--action <action>** Sets action to: 1 = GetCurrentStatus 2 = Enable 3 = Disable

4.5.3. System Management

System Management

Commands	Long Options
GetFruInfo	**--file <file name> (Optional)** Saves the dumped FRU data to a file. **--overwrite (Optional)** Overwrites the output file. **--dev_id <Device ID> (Optional)** Gets more FRUs from CMM. FRU ID: [1-19] or "ALL" 1 = CMM Master 2 = CMM Middle Plane 3 = CMM Switch(A1) 4 = CMM Switch(A2) 5 = CMM Switch(B1) 6 = CMM Switch(B2) 7 = CMM PSU(A1) 8 = CMM PSU(A2) 9 = CMM PSU(A3) 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 **--redfish (Optional)** Enables support for pure Redfish. **--showall (Optional)** Gets all FRU information from managed system. **--file_only (Optional)** Works with the --file option and only reads FRU information from the input dumped FRU binary file. **--format <file format> (Optional)** 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. **--dump (Optional)** Works with the --file option and dumps FRU data.

	--json_view (Optional) Sets the output format to JSON.
RestoreFruInfo	**--file <file name>** Reads dumped FRU file. **--individually (Optional)** Restores each BMC with corresponding FRU info file individually. **--format <file format> (Optional)** Works with the --fileoption Works with the --file option to read a FRU file inone of the following specified formats: BINARY = Binary format TEXT = Text format If the option --format is not provided, the default format is BINARY.
ChangeFruInfo	**--value <assignment value>** Updates the value of the given FRU field. If the item is ALL, the format is "<CT>,<CP>,<CS>,<BDT>,<BM>,<BPN>,<BS>,<BP>,<PM>,<PN>,<PPM>,<PV>,<PS>, <PAT>" **--item <item name>** 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 **--fru_version <FRU version>** Updates the FRU version.

GetSystemInfo	**--redfish (Optional)** Enables support for pure Redfish. **--json_view (Optional)** Sets the output format to JSON.
GetSystemCfg	**--file <file name> (Optional)** Saves the configuration to a file. **--file_id <file ID> (Optional)** Downloads existing Blade system profile from CMM with specific file ID. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--download (Optional)** Downloads current Blade system configuration file that support profile update from CMM. **--overwrite (Optional)** Overwrites the output file. **--dev_id <Device ID> (Optional)** Assigns Blade index and node ID. Blade index: [A1-A14] or [B1-B14] Node ID: [1-4] Format: [A1_1] **--action <action> (Optional)** Sets the action of each XML table. Acceptable option: None or Change. **--cur_pw_file <Current password file> (Optional)** The specified file path to read BIOS Administrator password.
ChangeSystemCfg	**--file <file name>** Updates the managed system with the given configuration file. **--file_id <file ID> (Optional)** Assigns profile ID using the ProfileManage command. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--upload (Optional)** Uploads the Blade system configuration file to the CMM for updating profiles.

	--update <update rule> (Optional) Updates Blade system configuration with the existing system profile on CMM. Supported update rule: [Apply] or [Deploy] **--skip_precheck (Optional)** Uploads and overwrites the existing system profile. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--dev_id <Device ID> (Optional)** 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 **--skip_unknown (Optional)** Skips the unknown settings or menus in the system configuration file. **--skip_bbs (Optional)** Skips the BBS-related menus in the BIOS configuration file. **--precheck (Optional)** Checks configuration before update. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--cur_pw_file <Current password file> (Optional)** The specified file path to read BIOS Administrator password.
GetFanMode	**--json_view (Optional)** Sets the output format to JSON.
SetFanMode	**--Fanmode <Fan Mode ID> (Optional)** Sets the selected FanMode type: 0 = Standard 1 = Full 2 = Optimal 3 = PUE2 Optimal 4 = Heavy IO 5 = PUE3 Optimal 6 = Liquid Cooling 7 = Smart

	8 = PUE Optimal 9 = Smart Cooling 10 = Performance 11 = Silent
LocateServerUid	**--action <action>** Sets action to: 1 = GetStatus 2 = On 3 = Off **--json_view <-c GetFanMode --json_view> (Optional)** Sets the output format to JSON.
GetFirmwareInventoryInfo	**--json_view (Optional)** Show the Firmware Inventory info in json format
ClearCMOS	**--ac_cycle** Proceeds with an AC cycle to the managed system after the operation. **--post_complete (Optional)** Waits for the managed system's POST to complete after AC power cycle.

4.5.4. BIOS Management

BIOS Management	
Commands	**Long Options**
UpdateBios	**--file <file name>** Updates the BIOS with the given BIOS image file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each BIOS with corresponding configuration file individually. **--flash_smbios (Optional)** Overwrites and resets the SMBIOS data. **--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.)

--redfish (Optional)
Enables support for pure Redfish.

--preserve_setting (Optional)
Preserves BIOS configurations.

--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 forward and upgrades to the next revision. (Only supported by the X12/H12 and later platforms except the H12 non-RoT systems.)

--staged <action> (Optional)
Sets action to:
1 = update : The update process will start at the next system boot.
2 = abort : Aborts the previously staged update task.
3 = getinfo : Check whether if there was any pending staged update task.

--post_complete (Optional)
Waits for the managed system POST 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.

--upgrade_only (Optional)
Firmware updates are only performed when the version is newer.

--check_reboot_required (Optional)

	Displays a warning message when a system reboot or power cycle is required.
GetBiosInfo	**--file <file name> (Optional)** Reads BIOS information from an input BIOS image file. **--individually (Optional)** Gets each BIOS with its corresponding image file individually. **--redfish (Optional)** Enables support for pure Redfish. **--showall (Optional)** Prints the BIOS version, BIOS revision and BIOS OEM FID information. **--file_only (Optional)** Works with --file, and only reads BIOS information from the input image file. **--extract_measurement (Optional)** Works with --file, extract BIOS image file measurement. **--json_view (Optional)** Sets the output format to JSON.
GetDefaultBiosCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the default factory BIOS configuration on the screen if the file-saving function is not available. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--overwrite (Optional)** Overwrites the output file. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password.
GetCurrentBiosCfg	**--file <file name> (Optional)** Saves the BIOS configuration to a file. Prints the current BIOS configuration on the screen if the file-saving function is not available. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password.

	--overwrite (Optional) Overwrites the output file. **--tui (Optional)** Edits BIOS configuration in text-based user interface. **--compact (Optional)** Generates a compact version of the BIOS configuration containing only the settings that have been changed in the text-based user interface. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password. **--filter <Filter type> (Optional)** Sets filter type to: 1 = nondefault
ChangeBiosCfg	**--file <file name>** Updates the BIOS with the given configuration file. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each BIOS with corresponding configuration file individually. **--skip_unknown (Optional)** Skips the unknown settings or menus in the BIOS configuration file. **--skip_bbs (Optional)** Skips the BBS-related menus in the BIOS configuration file. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password.
LoadDefaultBiosCfg	**--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--reboot (Optional)** Forces the managed system to reboot or power up after operation.

	--redfish (Optional) Enables pure Redfish support. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--clear_bios_eventlog (Optional)** Clears the BIOS event log. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password.
GetDmiInfo	**--json_view (Optional)** Sets the output format to JSON. **--file <file name> (Optional)** Saves the DMI information to a file. Prints the DMI information on the screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
EditDmiInfo	**--file <file name>** The DMI information file to be edited (or created if it does not exist). **--item_type <item type>** Specifies the item type. **--item_name <item name>** Specifies the item name. **--shn <short name>** Specifies the item in short name format. **--value <assignment value>** Assigns the value to the item. **--default** Assigns the default value to the item.
ChangeDmiInfo	**--file <file name>** Updates the DMI information with the given text file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation.

	--individually (Optional) Individually updates each piece of DMI information with its corresponding text file **--post_complete (Optional)** Waits for the managed system POST complete after rebooting.
SetBiosPassword	**--new_password <new password> (Optional)** Sets the new BIOS Administrator password. **--confirm_password <confirms password> (Optional)** Confirms the new BIOS Administrator password. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--pw_file <Password File> (Optional)** The specified file path to read new password. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password.
EraseOAKey	**--reboot (Optional)** Forces the managed system to reboot or power up after operation.
GetScpInfo	**--file <file name> (Optional)** Reads SCP information from an input SCP image file. **--file_only (Optional)** Works with --file, and only reads SCP information from the input image file. **--json_view (Optional)** Sets the output format to JSON.
UpdateScp	**--file <file name>** Updates SCP with the given FW image file.

	--reboot Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each SCP with corresponding firmware file individually. **--post_complete (Optional)** Waits until the managed system completes POST following a reboot.
GetFixedBootCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the BIOS fixed boot order configuration on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
GetBootOption	**--json_view (Optional)** Sets the output format to JSON.
SetBootOption	**--device_type <Device Type ID>** 0: No Override Sets the Device_Type to the following numbers for Legacy Device: 1: PXE 2: Hard Drive 3: CD DVD 4: BIOS Setup 5: USB Key 6: Virtual USB Hard Drive 7: Virtual Floppy 8: ISO Image Sets the Device_Type to the following numbers for UEFI Device 9: UEFI: Hard Drive 10: UEFI: CD DVD 11: UEFI: USB Key 12: Virtual UEFI: USB Hard Drive 13: UEFI: ISO Image 14: UEFI: PXE 15: UEFI: Floppy|Virtual Floppy 16: UEFI: BIOS Shell **--action <action> (Optional)** Sets power action with: 0 = up 1 = down

	2 = cycle 3 = reset 4 = softshutdown 5 = reboot 6 = accycle 7 = nmi 8 = on **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--next_boot_only <Enable/Disable> (Optional)** Sets NextBootOnly status for non-GB200 platforms Valid options are: - Enable: Enable the boot override. - Disable: Disable the boot override. The default value is Enable. **--boot_override_mode <Set boot override mode> (Optional)** Sets BootSourceOverride status in GB200 Valid options are: - Once: The boot override will be applied only once. - Continuous: The boot override will be applied continuously. - Disabled: The boot override is disabled. The default value is Once.
SetHttpBoot	**--file <file name> (Optional)** Upload the TLS certificate with type .cer,.der,.crt,.pem format. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--boot_name <boot description> (Optional)** Description for HTTP boot. **--boot_lan <boot LAN port> (Optional)** Enters the LAN port for HTTP boot. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--boot_clean (Optional)** Cleans all HTTP boot option. **--disable_hostname_check (Optional)** Disables checking whether the host name of the TLS certificate matches the host name provided by the remote server for HTTPS boot. **--image_url <URL> (Optional)**

	The URL to access the shared image file. URL format: 'http://<IPv4 or IPv6>/<shared point>/<file path>' or 'https://<IPv4 or IPv6>/<shared point>/<file path>' **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password.
ChangeFixedBootCfg	**--file <file name>** Updates the BIOS fixed boot order with the given configuration file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each BIOS fixed boot configuration with corresponding configuration file individually. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
GetBiosPostCode	**--json_view <-c command-name --json_view> (Optional)** Sets the output format to JSON.

4.5.5. BMC Management

BMC Management	
Commands	**Long Options**
UpdateBmc	**--file <file name>** Updates the BMC with the given BMC file. **--individually (Optional)** Updates each BMC with corresponding firmware file individually. **--overwrite_cfg (Optional)** Overwrites the current BMC configuration using the factory default values in the given BMC image file. **--overwrite_sdr (Optional)** Overwrites current BMC SDR data.

	--overwrite_ssl (Optional) Overwrites current BMC SSL configuration. (Only supported by the X12/H12 and later platforms except the H12 non-RoT systems.) **--redfish (Optional)** Enables support for pure Redfish. **--backup (Optional)** Backs up the current BMC image. (Only supported by the RoT systems.) **--forward (Optional)** Confirms the Rollback ID and upgrades to the next revision. (Only supported by the X12/H12 and later platforms except the H12 non-RoT systems.) **--bmc_boot_check (Optional)** Checks if BMC boots up within 16 minutes after update. (Only supported by the X12/H12 and later platforms except the H12 non-RoT systems.) **--upgrade_only (Optional)** Firmware updates are only performed when the version is newer. **--check_reboot_required (Optional)** Displays a warning message when a system reboot or power cycle is required. **--no_waiting (Optional)** Bypasses the standard waiting period after BMC firmware updates. Normally the tool waits for the BMC to complete its cold reset cycle before proceeding. This option skips the wait time but may cause connection failures if the BMC is still rebooting.
GetBmcInfo	**--file <file name> (Optional)** Reads the BMC information from an input BMC image file. **--individually (Optional)** Gets each BMC with its corresponding image file individually. **--redfish (Optional)** Enables support for pure Redfish. **--showall (Optional)** Display all information.

	--file_only (Optional) Works with --file option, and only reads BMC information from the input image file. **--extract_measurement (Optional)** Works with the --file option, and extracts BMC image file measurement. **--json_view (Optional)** Sets the output format to JSON.
GetBmcCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the BMC configuration on screen if the file-saving function is not available. **--sample_file <sample file> (Optional)** Creates BMC configuration using the format from the sample file. **--overwrite (Optional)** Overwrites the output file. **--action <action> (Optional)** Sets the action of each XML table. Acceptable option: None or Change. **--dump (Optional)** Dumps read-only BMC configuration file.
ChangeBmcCfg	**--file <file name>** Updates the BMC with the given configuration file. **--individually (Optional)** Updates each BMC with corresponding configuration file individually. **--skip_unknown (Optional)** Skips the unknown tables or settings in the BMC configuration file. **--restore (Optional)** Restores the BMC configuration with the corresponding read-only configuration file.
DownloadBmcCfg	**--file <file name>** Downloads the BMC configuration to a file.

	--overwrite (Optional) Overwrites the output file. **--format <file format> (Optional)** Works with the --file option to download the BMC configuration to a 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.
UploadBmcCfg	**--file <file name>** Uploads the BMC with the given configuration file. **--individually (Optional)** Uploads each BMC with corresponding configuration file individually. **--format <file format> (Optional)** Works with the --file option to upload BMC configuration from 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.
SetBmcPassword	**--user_id <user ID> (Optional)** Enters the BMC user ID. **--new_password <new password> (Optional)** Sets the new BMC user password. **--confirm_password <confirms password> (Optional)** Confirms the new BMC user password. **--pw_file <Password File> (Optional)** The specified file path to read the new BMC user password.
GetKcsPriv	**--json_view (Optional)** Sets the output format to JSON.
SetKcsPriv	**--priv_level <KCS Privilege level>** Sets KCS privilege with level. 1 = Call Back

	2 = User 3 = Operator 4 = Administrator
LoadDefaultBmcCfg	**--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--redfish (Optional)** Enables support for pure Redfish. **--clear_user_cfg (Optional)** Clears user configuration. **--preserve_user_cfg (Optional)** Preserves user configuration. **--load_unique_password (Optional)** Loads the unique BMC password. **--load_default_password (Optional)** Loads the default BMC password. **--load_default_lan (Optional)** Loads the default BMC LAN configuration. **--load_default_fru (Optional)** Loads the default FRU configuration. **--reset_all (Optional)** Loads default configuration for NVIDIA platforms. Different NVIDIA platforms may load different configurations depending on platform capabilities as following: - NVIDIA C2: Loads default BMC and BIOS configurations. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--bmc_boot_check (Optional)** Checks if BMC is booted up after reset.

BmcReset	**--action <action>** Sets action to: 1 = ColdReset 2 = WarmReset **--bmc_boot_check (Optional)** Checks BMC boots up within 4 minutes after reset.
GetBmcUserList	**--json_view <-c command-name --json_view> (Optional)** Sets the output format to JSON.
SetBmcUserList	**--action <action>** Sets action to: 1 = Add 2 = Del 3 = Level 4 = SetPwd 5 = Test 6 = EnableType 7 = EnableAccount 8 = EditUserName **--user_id <user ID> (Optional)** The BMC user ID. **--user_name <user name> (Optional)** The BMC user name. **--user_password <user password> (Optional)** The BMC user password. **--user_privilege <user privilege> (Optional)** The BMC user privilege. For privilege level: Administrator: 4 Operator : 3 User : 2 Callback : 1 No Access : 15 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)** Manages account type status. 0 = Disable 1 = Enable **--ap <authentication protocol> (Optional)** The authentication protocol. 0 = MD5 1 = SHA **--pp <private protocol> (Optional)** The private 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. The format is "SNMP:Enable,Redfish:Disable." Supported account types are: 1. Redfish 2. SNMP **--current_user_name <current user name> (Optional)** The current BMC username for user management operations (NVIDIA C2 specific).
BootStrappingAccount	**--action <action>** Sets action to: 1 = CreateAccount 2 = DeleteAccount 3 = CheckAccount **--user_name <user name> (Optional)** Delete bootstrapping account with user name.
RmcpManage	**--action <action>** Sets RMCP status with: 1 = GetInfo 2 = Enable

	3 = Disable **--port <port> (Optional)** Command optional port(s) The format is "RMCP:623" or "623". Command optional port(s) list: 1. RMCP (for RMCP service port)
BmcHostName	**--action <action>** Sets BmcHostName action to: 1 = Get 2 = Set **--hostname <Host Name> (Optional)** BMC Host name **--json_view <-c BmcHostName --action Get --json_view> (Optional)** Sets the output format to JSON.
GetSessionInfo	**--json_view (Optional)** Sets the output format to JSON.
ManageRHI	**--action <action>** Sets action to: 1 = GetConnection 2 = SetConnection **--type <type> (Optional)** Sets USB connection Supported connection type string: 0 = RNDIS 1 = CDC_ECM (Input type string will be converted to above type number)
BmcWatchDog	**--action <action>** Sets WatchDog actions to: 0 = Set 1 = Info 2 = Reset **--timer_action <Watchdog timer actions> (Optional)** Sets WatchDog timer actions to: 0 = NoAction 1 = HardReset

	2 = PowerDown 3 = PowerCycle **--interval <time interval> (Optional)** Sets WatchDog pre-timeout interval in seconds **--countdown <Watchdog count down> (Optional)** Sets WatchDog initial count down value
SnmpManage	**--action <action>** Sets action to: 1 = GetStatus 2 = On 3 = Off 4 = GetCommunityString 5 = SetCommunityString **--snmp_id (Optional)** Assigns SNMP index. SNMP index: [1-15] **--snmp_ip (Optional)** Sets SNMP IP **--snmp_mac (Optional)** Sets SNMP MAC address **--community_string (Optional)** Sets SNMP community string
BmcIPv6StaticRouteManage	**--action <action>** Sets action to: 1 = GetInfo 2 = Enable 3 = Disable 4 = SetStaticRoute 5 = Clear **--ipv6_ip <IPv6 IP> (Optional)** Specifies the IPv6 IP address for configuration. **--ipv6_prefix_value <IPv6 prefix value> (Optional)** Specifies IPv6 prefix value for configuration. **--ipv6_prefix_len <IPv6 prefix length> (Optional)** Specifies the IPv6 prefix length for configuration.

	--router_id <Router ID> (Optional) Specifies an IPv6 router for configuration. The value is 1 or 2.
SessionManage	**--action <action>** Sets action to: 1 = GetInfo 2 = Disconnect **--session_id <SESSION ID> (Optional)** Specifies the session with the given session ID.

4.5.6. System Event Log

System Event Log	
Commands	**Long Options**
GetEventLog	**--json_view (Optional)** Sets the output format to JSON. **--file <file name> (Optional)** Saves the event log to a file. Prints the event log on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file. **--redfish (Optional)** Enables pure Redfish support. **--info (Optional)** Print the current and total capacity of event log. **--raw_data (Optional)** Prints the raw data of each event log. **--mfg (Optional)** Prints the general information of event logs for the managed system in a style that complies with the manufacturer's assembly line requirements. **--year <year> (Optional)** Filter event logs within n years **--month <month> (Optional)** Filter event logs within n months

	--day <day> (Optional) Filter event logs within n days **--format <file format> (Optional)** Saves the event log to a file in CSV format.
ClearEventLog	**--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot. **--clear_bmc_eventlog (Optional)** Only clears the BMC event log. **--clear_bios_eventlog (Optional)** Only clears the BIOS event log. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password.
GetMaintenEventLog	**--file <file name> (Optional)** Saves the Maintenance Event Log to a file. Prints the Maintenance Event Log on screen if the file-saving function is not available. **--st <start time> (Optional)** Enters the start time YYYYMMDD. **--et <end time> (Optional)** Enters the end time YYYYMMDD. **--count <Count> (Optional)** Enters the log count. If count number equal zero will show all. **--overwrite (Optional)** Overwrites the output file. **--json_view <-c command-name --json_view> (Optional)** Sets the output format to JSON.

ClearMaintenEventLog	**--gen_log (Optional)** Generates a log entry indicating the successful clearing of the maintenance event log.
GetHostDump	**--action <action>** Sets action to: 1 = CreateDump 2 = DeleteDump 3 = DirectDump **--file <file name> (Optional)** Saves the crash dump to a file. **--overwrite (Optional)** Overwrites the output file.
SetSELTimeMode	**--time <Time>** Sets the managed system SEL time [YYYYMMDDhhmmss]/[YYYYMMDDhhmm].
GetPostCodeLog	**--file <file name> (Optional)** Saves the post code log to a file. Prints the post code log on screen if the file-saving function is not available. **--file_type <file type> (Optional)** Saves the file as a specific type. Supported type: JSON **--st <start time> (Optional)** Enters the start time YYYYMMDD. **--et <end time> (Optional)** Enters the end time YYYYMMDD. **--count <Count> (Optional)** Specifies the number of logs to display (range: 1-999). **--overwrite (Optional)** Overwrites the output file.
ClearPostCodeLog	None

4.5.7. CMM Management

CMM Management (OOB Only)	
Commands	**Long Options**
UpdateCmm	**--file <file name>** Updates the CMM with the given image file. **--individually (Optional)** Updates each CMM with its corresponding image file individually. **--overwrite_cfg (Optional)** Overwrites the current CMM configurations, including network settings, using the default factory values in the given CMM image file. This might cause the IPMI connection to be lost. **--overwrite_sdr (Optional)** Overwrites the current CMM SDR data. **--overwrite_ssl (Optional)** Overwrites the current CMM SSL configuration. **--backup (Optional)** Backs up the current CMM image. (Only supported by the RoT systems.) **--cmm_boot_check (Optional)** Checks if the CMM has booted up after a reset.
GetCmmInfo	**--file <file name> (Optional)** Reads the CMM information from an input CMM image file. **--individually (Optional)** Gets each CMM with its corresponding image file individually. **--showall (Optional)** Prints BIOS, BMC and ARM SAA information of the managed Blade system. **--file_only (Optional)** Works with option --file, and only reads CMM information from the input image file. **--json_view (Optional)** Sets the output format to JSON.

GetCmmCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the CMM configuration on screen if the file-saving function is not available. **--download (Optional)** Downloads the current CMM configuration file that supports profile update from CMM. **--profile_repo (Optional)** Downloads existing CMM profile from CMM. **--overwrite (Optional)** Overwrites the output file. **--action <action> (Optional)** Sets the action of each XML table. Acceptable option: None or Change.
ChangeCmmCfg	**--file <file name>** Updates the CMM with the given configuration file. **--upload (Optional)** Uploads the CMM configuration file to CMM for updating profiles. **--update <update rule> (Optional)** Updates CMM configuration with the existing profile on CMM. Supported update rule: [Apply] **--skip_precheck (Optional)** Uploads and overwrites the existing CMM profile. **--individually (Optional)** Updates each CMM with corresponding configuration file individually. **--skip_unknown (Optional)** Skips the unknown tables or settings in the CMM configuration file. **--precheck (Optional)** Checks configuration before update.
SetCmmPassword	**--user_id <user ID> (Optional)** Enters the CMM user ID. **--new_password <new password> (Optional)** Sets the new CMM user password. **--confirm_password <confirms password> (Optional)**

	Confirms the new CMM user password. **--pw_file <Password File> (Optional)** The specified file path to read the new CMM user password.
LoadDefaultCmmCfg	**--clear_user_cfg (Optional)** Clears user configuration. **--preserve_user_cfg (Optional)** Preserves user configuration. **--load_unique_password (Optional)** Loads CMM unique password. **--load_default_password (Optional)** Loads CMM default password.
GetBbpInfo	**--file <file name> (Optional)** Reads the BBP information from an input BBP image file. **--file_only (Optional)** Works with --file, and only reads BBP information from the input image file. **--json_view (Optional)** Sets the output format to JSON.
UpdateBbp	**--file <file name>** Updates the BBP with the given image file. **--skip_check (Optional)** Skips the Blade power status check to force update BBP
GetBladePowerStatus	**--json_view (Optional)** Sets the output format to JSON.
SetBladePowerAction	**--action <action>** Sets power action with: 0 = down 1 = up 2 = cycle 3 = reset 5 = softshutdown 24 = accycle

	--Blade <Blade Index> Assigns Blade index. [A1-A14], [B1-B14] or ALL **--node <Node Index> (Optional)** Assigns node index. [1-4]
ProfileManage	**--action <action>** Supported actions: Get, Edit and Delete. **--file <file name> (Optional)** Saves the profile list to a file. Prints the profile list on the screen if the file-saving function is not available. **--file_id <file ID> (Optional)** Gets and edits profile information or deletes the profile on CMM with the specific file ID **--profile_name <profile name> (Optional)** Edits the profile name of the specified profile on CMM with the specific file ID. **--profile_description <profile description> (Optional)** Edits the profile description of the specified profile on CMM with the specific file ID. **--schedule_update_time <schedule update time> (Optional)** Edits the scheduled update time of the specified profile on CMM with the specific file ID. Format: [YYYY-MM-DD_HH:MM] **--overwrite (Optional)** Overwrites the output file. **--showall (Optional)** Gets the profile association information between the specified profile and selected Blade systems with a specific profile ID.
BladePsuManage	**--action <action>** Manages system with action: GetBladePsuInfo GetBladePsuConsumption GetFanSpeed SetFanSpeed GetFanMode

	SetFanMode **--index <index> (Optional)** Assigns PSU index or Fan index. PSU index: [A1-A4] or [B1-B4] Fan index: [C1-C3] **--json_view (Optional)** Sets the output format to JSON. **--value <assignment value>** Assigns fan speed level. Speed level: [1-10]
BladeSummary	None
BladeConsole	**--blade_id <blade ID>** Specifies the blade ID. **--node_id <node ID>** Specifies the node ID.
GetCmmUserList	**--json_view <-c command-name --json_view> (Optional)** Sets the output format to JSON.
SetCmmUserList	**--action <action>** Sets action to: 1 = Add 2 = Del 3 = Level 4 = SetPwd 5 = Test 6 = EnableType **--user_id <user ID> (Optional)** The CMM user ID. **--user_name <user name> (Optional)** The CMM user name. **--user_password <user password> (Optional)** The CMM user password. **--user_privilege <user privilege> (Optional)** The CMM user privilege.

	For privilege level: Administrator: 4 Operator : 3 User : 2 Callback : 1 No Access : 15 The "No Access" privilege level is not supported after AST2600 platform **--account_type <account type> (Optional)** Supported account types for CMM 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 private protocol. 0 = DES 1 = AES **--ak <authentication key> (Optional)** The authentication key. **--pk <private key> (Optional)** The private key.
UpdateDummySwitch	**--file <file name> (Optional)** Updates the CMM dummy switch with the given image file. **--upload (Optional)** Uploads the CMM dummy switch with the given image file only. **--update <update rule> (Optional)** Updates CMM dummy switch with the existing image on CMM. Supported update rule: [Apply] **--individually (Optional)** Updates each CMM dummy switch with its corresponding image file individually.

BladeNodeManage	**--action <action>** Manages the nodes of the Blade system with action: GetSensor GetStatus GetPower SetPower GetIp SetIp GetDhcp SetDhcp GetMac SetMac GetSubnetMask SetSubnetMask GetGateway SetGateway GetName SetName GetUid SetUid GetSystemModel **--blade_id <blade ID> (Optional)** Specifies the blade ID. **--node_id <node ID> (Optional)** Specifies the node ID. **--value <value>** Specifies the power state. 0: Power Off 1: Power On 2: Power Cycle 3: Power Reset 4: AC cycle 5: Graceful-shutdown

4.5.8. Storage Management

Storage Management	
Commands	**Long Options**
GetRaidControllerInfo	**--file <file name> (Optional)** Reads the RAID controller firmware information from an input RAID image file. **--controller <Controller> (Optional)**

	<Broadcom/Marvell> Vendor of RAID controller. **--dev_id <Device ID> (Optional)** RAID controller device ID. **--file_only (Optional)** Works with --file, and only reads RAID controller firmware information from the input image file. **--json_view (Optional)** Sets the output format to JSON.
UpdateRaidController	**--file <file name>** Updates the RAID controller with the given RAID file. **--controller <Controller>** <Broadcom/Marvell> Vendor of RAID controller. **--dev_id <Device ID>** Device ID of RAID controller. **--type <type>** Specifies RAID type for Broadcom devices. Supported types: HBA HA-RAID **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--upgrade_only (Optional)** Firmware updates are only performed when the version is newer. **--check_reboot_required (Optional)** Displays a warning message when a system reboot or power cycle is required.
GetRaidCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the RAID configuration on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.

	--controller <Controller> (Optional) <Broadcom/Marvell> Vendor of RAID controller.
ChangeRaidCfg	**--file <file name>** Updates the RAID with the given configuration file. **--individually (Optional)** Updates each RAID with corresponding configuration file individually. **--controller <Controller> (Optional)** <Broadcom/Marvell> Vendor of RAID controller.
GetSataInfo	**--json_view (Optional)** Sets the output format to JSON.
GetNvmeInfo	**--json_view (Optional)** Sets the output format to JSON. **--dev_id <Device ID> (Optional)** NVMe device controller ID. Prints all NVMe information on the screen if this option is not available. **--redfish (Optional)** Enables pure Redfish support.
GetPMemInfo	**--file <file name> (Optional)** Reads the PMem information from an input PMem image file. **--file_only (Optional)** Works with the --file option, and only reads PMem information from the input image file. **--json_view <-c GetPMemInfo --json_view> (Optional)** Sets the output format to JSON.
UpdatePMem	**--file <file name> (Optional)** Updates PMem with the given PMem firmware file. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--reboot (Optional)** Forces the managed system to reboot or power up after operation.

	--restore_default_fw (Optional) Updates the PMem with BIOS built-in PMem firmware. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password.
GetVROCCfg	**--file <file name> (Optional)** Saves the configuration to a file. Prints the VROC configuration on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.
ChangeVROCCfg	**--file <file name>** Updates the VROC with the given configuration file. **--individually (Optional)** Updates each VROC with corresponding configuration file individually.
ControlNVMe	**--dev_id <Device ID>** The NVMe controller ID can be found using the GetNvmeInfo command. **--action <action>** Sets action to: 1 = Locate 2 = StopLocate 3 = Insert 4 = Remove 5 = Rescan **--group_id <Group ID>** The NVMe device group ID can be found using the GetNvmeInfo command. **--slot <Slot number>** The NVMe slot number can be found using the GetNvmeInfo command. **--no_eject <eject option> (Optional)** Setting the eject option. The default value is 'eject'.

	--device_name <HDD Name> (Optional) The NVMe device name, can be found with GetNvmeInfo and GetSmartData command.
GetSmartData	**--json_view (Optional)** Sets the output format to JSON. **--device_name <HDD Name> (Optional)** Gets the specific device smart data
GetSasExpanderInfo	**--file <file name> (Optional)** Reads the SAS Expander information from an input image file. **--file_only (Optional)** Works with the --file option, and only reads SAS Expander information from the input image file. **--json_view (Optional)** Sets the output format to JSON.
UpdateSasExpander	**--file <file name>** Updates SAS Expander with the given image file. **--index <index>** Set the SAS Expander index that needs to be updated. **--reboot (Optional)** Forces the managed system to power cycle after operation.

4.5.9. Power Management

Power Management	
Commands	**Long Options**
GetPsuInfo	**--json_view (Optional)** Sets the output format to JSON.
UpdatePsu	**--file <file name> (Optional)** PSU firmware file **--reboot (Optional)**

	Forces the managed system to reboot or power up after operation. **--address (Optional)** PSU module address in HEX format (Gets the PSU module slave address from the GetPSUInfo command.) **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--index <index> (Optional)** PSU module index (Gets the PSU module index from the GetPSUInfo command.)
GetPowerStatus	**--json_view (Optional)** Sets the output format to JSON.
SetPowerAction	**--action <action>** Sets power action with: 0 = up 1 = down 2 = cycle 3 = reset 4 = softshutdown 5 = reboot 6 = accycle 7 = nmi 8 = on **--interval <time interval> (Optional)** Set power cycle interval in seconds. **--post_complete (Optional)** Waits for the managed system POST to complete after rebooting. **--power_on (Optional)** Powers on the system after AC cycle.
DcmiManage	**--type <type>** Manages system with type: STD_DCMI NM20 **--start_ip <Start IP> (Optional)** Specifies IPv4 IP address. **--end_ip <End IP> (Optional)** Specifies IPv4 IP address.

	--netmask <Netmask> (Optional) Specifies netmask. **--json_view (Optional)** Sets the output format to JSON. **--period <Period> (Optional)** Specifies rolling average time period. Please execute DcmiManage command with --type NM20 and --action GetCap to get supported period(hex value). **--action <action>** Manages system with action: Find GetCap GetPowerStatus GetMCID SetMCID GetAssetTag SetAssetTag **--value <assignment value>** Specifies MCID string value. **--mode <Mode>** Specifies power reading mode. 1: System Power Statistics 2: Enhanced System Power Statistics **--limit <limit>** Specifies power limit in watts. **--exception_action <Exception action>** Specifies exception action 0: No Action 1: Hard power off system and log event to SEL 17: Log event to SEL **--time <Time>** Specifies correction time limit in milliseconds.
PowerPolicy	**--type <type>** Manages power policy with type: NM20 BMC10 **--json_view (Optional)** Sets the output format to JSON.

--overwrite (Optional)
Overwrites the policy.

--domain_id <Domain ID> (Optional)
0: Entire platform
1: CPU subsystem
2: Memory subsystem
3: HW Protection
4: High power I/O subsystem
If the --domain_id option is not provided, sets the domain ID to Entire platform by default.

--value <assignment value> (Optional)
Specifies threshold value.
Up to three threshold values, and each threshold is separated by commas(,).

--st <start time> (Optional)
Policy suspension start time (HHmm) [0000~2359]

--et <end time> (Optional)
Policy suspension end time (HHmm) [0006~2400]
If there is a need to specify an end-time that is beyond midnight, use two suspension periods.

--days <Days> (Optional)
Recurrence of the suspension period
1 - Monday, 2 - Tuesday, 3 - Wednesday, 4 - Thursday
5 - Friday, 6 - Saturday, 7 - Sunday
ex: every Monday, Wednesday, Sunday => 137

--mode <Mode> (Optional)
Specifies aggressive CPU power correction mode.
0: Automatic mode
1: Force non-aggressive mode
2: Force aggressive mode
If the --mode option is not provided, the default mode is Automatic mode.

--action <action>
Manages power policy with action:
EnableGlobal
DisableGlobal
EnableDomain
DisableDomain
EnablePolicy
DisablePolicy
AddPowerPolicy
GetPolicy
DelPolicy

ScanPolicy
AddPolicy
GetAlertThreshold
SetAlertThreshold
GetPeriod
AddPeriod
UpdatePeriod
DeletePeriod
ClearPeriod

--policy_id <Policy ID>
Specifies policy ID from 0 to 255.

--limit <limit>
Specifies policy target limit.

--period <Period>
Specifies statistics reporting period in seconds.

--time <Time>
Specifies correction time limit (ms).

--exception_action <Exception action>
Specifies policy exception action.
1: Send alert
2: Shutdown system
3: Send alert and shutdown system

--trigger_type <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: MGPIO policy trigger

--trigger_limit <Trigger limit>
Specifies policy trigger limit.

--count <Count>
Specifies count.
0: Clear all thresholds
[1-3]: Number of alert thresholds

--period_id <Period ID>
Period ID 1~5 for which policy should be used

--storage <Storage>
Specifies storage option.

	0: Persistent storage 1: Volatile memory
GetAcpiPowerStatus	None
GetAiomStandbyPower	None
SetAiomStandbyPower	**--action <action>** Sets action to: 1 = On 2 = Off
CpuPowerManage	**--value <assignment value>** Assigns a power limit value. **--action <action>** Sets action with: 1 = GetPowerLimit 2 = SetPowerLimitEnabled 3 = SetPowerLimitDisabled **--redfish (Optional)** Enables support for pure Redfish.
GetPowerShelfInfo	**--json_view (Optional)** Sets the output format to JSON. **--dev_id <Device ID> (Optional)** Specifies the device ID to retrieve information for a single power unit. Supported values: [0–5].
UpdatePowerShelf	**--dev_id <Device ID>** Specifies the device ID used to designate which power unit will be updated. Supported values: [0–5]. **--file <Firmware File Name>** Specifies the firmware file, including the path

4.5.10. Applications

Applications	
Commands	**Long Options**
RawCommand	**--raw <raw command> (Optional)** Input hex-value commands. **--ipmb <IPMB command> (Optional)** Input hex-value commands.
GetUsbAccessMode	None
SetUsbAccessMode	**--panel <front/rear>** The panel to be set **--enable (Optional)** Dynamically enables the USB ports in the assigned panel. **--disable (Optional)** Dynamically disables the USB ports in the assigned panel.
KmsManage	**--port <port> (Optional)** Command optional port(s) The format is "TCP:5696" or "5696" Command optional port(s) list: 1. TCP (for KMS server port) **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--action <action> (Optional)** Sets KMS manage action to: 1 = GetInfo 2 = Probe 3 = DeleteCA 4 = DeleteCert 5 = DeletePvtKey 6 = DeleteAll **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password.

	--server_ip <server IP address> (Optional) Enters KMS server IP address. **--second_server_ip <second server IP address> (Optional)** Enters second KMS server IP address. **--time_out <time out> (Optional)** Enters KMS server connecting time-out. **--time_zone <timezone> (Optional)** Enters correct time zone GMT+. **--client_username <client username> (Optional)** Enters client identity: UserName. **--client_password <client password> (Optional)** Enters client identity: Password. **--ca_cert <CA certificate file name> (Optional)** Uploads CA certificate from the file. **--client_cert <client certificate file name> (Optional)** Uploads client certificate from the file. **--pvt_key <private key file name> (Optional)** Uploads client private key from the file. **--pvt_key_pw <private key password> (Optional)** Enters client private key password.
RedfishApi	**--api <API path>** Redfish API path. **-v (Optional)** Verbose output: prints the response header. **--file <file name> (Optional)** Outputs the result to file. **--overwrite (Optional)** Overwrites the output file. **--individually (Optional)** Reads the request body from the file individually. (Only support for Multiple systems OOB usage) **--json_view (Optional)** Only display command output in json format without any informative/warning messages. If there's any error thenerror message

	will be displayed that wont be in json format.Using along with --no_banner output result in json format. **--request <HTTP method> (Optional)** HTTP method (GET, POST, PATCH) **--data <Request body> (Optional)** Request body. **--retry <Number of retry> (Optional)** Number of retry, default is 3. **--multipart <multipart/form-data> (Optional)** each multipart/form-data should be joined by && --multipart 'UpdateParameters={"Targets": ["/redfish/v1/Managers/1"], "@Redfish.OperationApplyTime": "Immediate"} && UpdateFile=@BMC_X13AST2600-F201MS_20240308_01.02.01_STDsp.bin
RemoteExec	**--remote_cmd <Remote command>** Enters the commands to be executed on a remote system. **--file <file name> (Optional)** Transfers the file(s) to a remote system.
RemoteConsole	None
RemoteScreenshot	**--file <file name>** Saves the screenshot to a file. **--overwrite (Optional)** Overwrites the output file.
RemoteKeyboard	**--file <file name> (Optional)** Reads keyboard operations from specified file. **--showall (Optional)** Shows all supported keys and some samples.
Sol	**--action <action>** Sets action to: 1 = Activate 2 = Deactivate 3 = GetInfo

	4 = Set **--value <assignment value> (Optional)** Assigns the value to the item. (Only supported with the 'Set' action.) **--channel <channel> (Optional)** Assigns the SOL channel. **--item <item name> (Optional)** Sets the SOL item value for the given SOL item. (Only supported with the 'Set' action.) 1 = set-in-progress Available values: [set-complete|set-in-progress|commit-write] 2 = enabled Available values: [true|false] 3 = privilege-level Available values: [user|operator|admin|oem] 4 = force-encryption Available values: [true|false] 5 = force-authentication Available values: [true|false] 6 = character-accumulate-level Available values: Integer, in 5 ms increments 7 = character-send-threshold Available values: Integer 8 = retry-count Available values: Integer 9 = retry-interval Available values: Integer, in 10 ms increments 10 = non-volatile-bit-rate Available values: [serial|9.6|19.2|38.4|57.6|115.2] 11 = volatile-bit-rate Available values: [serial|9.6|19.2|38.4|57.6|115.2]
FindBmcDevices	**--file <file name> (Optional)** The file to write, required with --getMACs used **--start_ip <Start IP> (Optional)** Start address of the network to search. **--end_ip <End IP> (Optional)** End address of the network to search. **--netmask <Netmask> (Optional)** Subnet mask of the network to search **--getMACs <Get the MAC addresses of available BMC devices> (Optional)** Retrieves the MAC addresses of the found BMC devices and

	writesthem to a file. **--find_user <Username for found device> (Optional)** Specifies the username for the found BMC devices. This optionshould be used in conjunction with the --getMACs option. **--find_password <Password for found device> (Optional)** Specifies the password for the found BMC devices. This optionshould be used in conjunction with the --getMACs option.
FoundBmcDevices	**--action <action>** Sets action to: 1 = List 2 = Clear 3 = Copy 4 = CopyAll 5 = SaveAs 6 = Refresh **--file <file name> (Optional)** The file to write, required with action "saveAs" used **--index <index> (Optional)** The indices of the host to copy, required with action "Copy" used
Shell	None
Prompt	**--item <item name>** 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 **--action <action>** Sets action to: 1 = Get 2 = Set **--enable (Optional)** Enables the the prompt value for the specified prompt item.

	--disable (Optional) Disables the the prompt value for the specified prompt item.
Ch	**--user_name <user name> (Optional)** Changes or adds a managed system with the specified username. **--user_password <user password> (Optional)** Changes or adds a managed system with the specified password. **--index <index> (Optional)** Switches to the managed system with the specified index. **--remove (Optional)** Removes the managed system with the specified index. **--host_ip <Host IP> (Optional)** Changes or adds the managed system's IP address.
RemoteScreenVideo	**--action <action>** Sets action to: 1 = Download 2 = Enable 3 = Disable **--period <period> (Optional)** Sets period to: 1 = BufferFull 2 = POSTEnd **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot. **--file <file name> (Optional)** Saves the screen recording to a file using the specified name. **--overwrite (Optional)** Overwrites the output file.

4.5.11. GPU Management

GPU Management

Commands	Long Options
GetGpuInfo	**--file <file name> (Optional)** Reads the GPU information from an input GPU image file. **--showall (Optional)** 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.) **--file_only (Optional)** Works with --file, and only reads GPU information from the input image file. **--showoam <Display Selected OAM> (Optional)** For Intel PVC and Intel Gaudi2/3 system shows individual OAM.
UpdateGpu	**--file <file name>** Updates the GPU firmware file that matches the FW item types. **--item <item name>** FW item types of GPU firmware: 1 = CEC 2 = FPGA 3 = HGX 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 = GAUDI_UBB_CPLD2 14 = HGX_FPGA 15 = HGX_HMC 16 = HGX_HMC_EROT 17 = HGX_FPGA_EROT 18 = HGX_PCIESWITCH 19 = HGX_PCIESWITCH_EROT 20 = HGX_GPU 21 = HGX_GPU_EROT 22 = HGX_NVSWITCH 23 = HGX_NVSWITCH_EROT 24 = HGX_RETIMER 25 = MGX_GPU 26 = MI300X 27 = ONBOARD_RETIMER

	28 = HGX_NVLINKMANAGEMENTNIC 29 = HGX_NVLINKMANAGEMENTNIC_EROT 30 = HGX_GPU_INFOROM 31 = HGX_CPLD 32 = HGX_CPU 33 = HGX_CPU_EROT **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--force_update (Optional)** update. **--dev_id <Device ID> (Optional)** Retrieved Device ID with the GetGPUInfo command. For SPI-FW, use the device Address. For HGX Retimer, HGX GPU, HGX GPU ERoT, HGX NVSwitch, HGX NVSwitch ERoT, and OnBoard Retimer, use the device id. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting.
DiagGpuStatus	**--dev_id <Device ID> (Optional)** The device ID list of GPU on the managed system.
GetGpuLog	**--file <file name>** Saves the GPU log to a file. **--item <item name>** Item type of GPU: 1 = HGX 2 = MI300X **--type <type>** Download type of GPU: 1 = DebugToken This option is only used for downloading Debug Token certificate log file. **--overwrite (Optional)** Overwrites the output file.
GpuPowerManage	**--value <assignment value>** Assigns power limit value. **--item <item name>** Item type of GPU:

	1 = HGX **--dev_id <Device ID>** GPU SXM Device ID can consist with multiple numbers, ranging from 1 to 8 (separate by comma), or All. **--action <action>** Sets action with: 1 = GetPowerLimit 2 = SetPowerLimit

4.5.12. CPLD Management

CPLD Management	
Commands	**Long Options**
GetCpldInfo	**--file <file name> (Optional)** Reads the CPLD information from an input CPLD image file. **--individually (Optional)** Gets each CPLD with its corresponding image file individually. **--file_only (Optional)** Works with the --file option, and only reads CPLD information from the input image file. **--extract_measurement (Optional)** Works with the --file option, extract CPLD image file measurement. **--json_view (Optional)** Sets the output format to JSON.
UpdateCpld	**--file <file name>** Updates the CPLD with the given CPLD image file. **--reboot** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each CPLD with its corresponding configuration file individually. **--post_complete (Optional)** Waits for the managed system's POST to complete after

	rebooting. **--index <index> (Optional)** Updates the CPLD with the given index. The default value is empty, and the first CPLD will be updated. **--poweroff (Optional)** Forces the managed system to power off during the update operation.
GetSwitchboardCpldInfo	**--file <file name> (Optional)** Reads the Switchboard CPLD information from an input image file. **--file_only (Optional)** Works with the --file option, and only reads Switchboard CPLD information from the input image file.
UpdateSwitchboardCpld	**--file <file name>** Updates the Main or Side Switchboard CPLD with the given image file. **--type <type>** Sets action to: 1 = Main 2 = Left 3 = Right **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each CPLD Switch Board with its corresponding configuration file individually. **--post_complete (Optional)** Waits for the managed system's POST to complete after rebooting. **--index <index> (Optional)** Sets the CPLD index. The default value is 1, and the index count starts from 1.
GetBackplaneCpldInfo	**--json_view (Optional)**

	Sets the output format to JSON.
UpdateBackplaneCpld	**--file <file name>** Updates the Backplane CPLD with the given FW image file. **--manual_ejected** Confirmed that all drives on backplane have been ejected manually. **--reboot (Optional)** Forces the managed system to power cycle after operation. **--individually (Optional)** Updates each backplane CPLD with its corresponding configuration file individually. **--index <index> (Optional)** Updates the specific Backplane CPLD with the given index. **--dev_id <Device ID> (Optional)** Sets the CPLD index. The default value is 1. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot. **--update_list <index:file name> (Optional)** Update multiple backplane CPLDs in one command, and use "," to distinguish items. **--upgrade_only (Optional)** Firmware updates are only performed when the version is newer. **--check_reboot_required (Optional)** Displays a warning message when a system reboot or power cycle is required.
GetFanboardCpldInfo	None
UpdateFanboardCpld	**--file <file name>** Updates the Fanboard CPLD with the given Fanboard CPLD image file. **--type <type>** Sets action to: 1 = Front 2 = Rear

	or the corresponding Fanboard ID number. **--individually (Optional)** Updates each Fanboard CPLD with the corresponding configuration file individually. **--index <index> (Optional)** Sets the CPLD index. The default value is 1, and the index count starts from 1.
GetAipCpldInfo	None
UpdateAipCpld	**--file <file name>** Updates the CPLD of AIP with the given FW image file. **--individually (Optional)** Updates each AIP CPLD with its corresponding image file individually.
GetAomboardCpldInfo	**--file <file name> (Optional)** Reads the CPLD information from an input AOM image file. **--file_only (Optional)** Works with the --file option, and only reads AOM information from the input image file. **--json_view (Optional)** Sets the output format to JSON.
UpdateAomboardCpld	**--file <file name>** Updates the AOM board with the given CPLD image file. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each AOM board CPLD with its corresponding image file individually. **--dev_id <Device ID> (Optional)** Updates the AOM board CPLD with the given AOM device ID. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.

	--index <index> (Optional) Updates the CPLD with the given index. The default value is empty, and the first CPLD on the AOM board will be updated. **--aom_type <aom type> (Optional)** Sets AOM type to update, the default value is "AOMboard": - AOMboard - AOM_SCM - AOM_PDB - AOM_FAN - AOM_M2 - AOM_RSC - or other supported AOM type string. **--poweroff (Optional)** Forces the managed system to power off during the update operation.
GetMiscCpldInfo	**--json_view (Optional)** Sets the output format to JSON.
UpdateMiscCpld	**--file <file name>** Updates the motherboard Miscellaneous CPLD with the given CPLD image file. **--reboot** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each motherboard Miscellaneous CPLD with its corresponding image file individually.
GetMidplaneSbbCpldInfo	**--json_view (Optional)** Sets the output format to JSON.
UpdateMidplaneSbbCpld	**--file <file name>** Updates the Midplane SBB CPLD with the given CPLD image file. **--reboot** Forces the managed system to reboot or power up after operation.

	--index <index> Sets CPLD index. **--individually (Optional)** Updates each Midplane SBB CPLD with its corresponding image file individually. **--post_complete (Optional)** Waits for the managed system POST complete after rebooting.
GetNICCpldInfo	None
UpdateNICCpld	**--file <file name>** Updates the NIC CPLD with the given CPLD image file. **--individually (Optional)** Updates each CPLD on NIC with its corresponding image file individually. **--dev_id <Device ID> (Optional)** 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	**--file <file name>** Updates the Transitionboard CPLD with the given CPLD image file. **--individually (Optional)** Updates each Transitionboard CPLD with corresponding image file individually.

4.5.13. NIC Management

NIC Management	
Commands	**Long Options**
UpdateAocNIC	**--file <file name>** Updates AOC NIC with the given add-on NIC file.

	--dev_id <Device ID> Device ID of AOC NIC. **-I <InterfaceName> (Optional)** <Redfish_HI> Uses Redfish Host Interface for in-band update. (Only support for in-band usage) **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot. **--upgrade_only (Optional)** Firmware updates are only performed when the version is newer. **--check_reboot_required (Optional)** Displays a warning message when a system reboot or power cycle is required.
GetAocNICInfo	**--file <file name> (Optional)** Reads the AOC NIC firmware information from an input AOC_NIC image file. **--dev_id <Device ID> (Optional)** AOC NIC device ID list. **--file_only (Optional)** Works with the --file option, and only reads AOC-NIC information from the input image file.

4.5.14. VM Management

VM Management	
Commands	**Long Options**
MountIsoImage	**--image_url <URL>** The URLs to access the shared image file. SAMBA URL: 'smb://<hostname or IP>/<shared point>/<file path>' SAMBA UNC: '\<hostname or IP><shared point><file path>' HTTP URL: 'http://<hostname or IP>/<shared point>/<file path>' HTTPS URL: 'https://<hostname or IP>/<shared point>/<file path>' **--id <ID> (Optional)** The specified ID to access the shared file.

	--pw <Password> (Optional) The specified password to access the shared file. **--pw_file <Password File> (Optional)** The specified file path to read password. **--redfish (Optional)** Enables support for pure Redfish.
UnmountIsoImage	**--redfish (Optional)** Enables support for pure Redfish.
MountFloppyImage	**--file <file name>** Mounts the specified binary floppy file to the managed system.
UnmountFloppyImage	None
GetVmInfo	**--dev_id <Device ID> (Optional)** The specified device ID to get virtual media information. The supported device ID: [1-3] **--redfish (Optional)** Enables pure Redfish support.
VmManage	**--action <action>** Sets action to: 1 = Enable 2 = Disable 3 = Mount 4 = Unmount **--port <port> (Optional)** Command optional port(s) The format is 'VM:623' or '623'. Command optional port(s) list: 1. VM (for virtual media port) **--image_url <URL> (Optional)** The URLs to access the shared image file. SAMBA URL: '<hostname or IP>/<shared point>/<file path>' HTTP URL: 'http://<hostname or IP>/<shared point>/<file path>' HTTPS URL: 'https://<hostname or IP>/<shared point>/<file path>' **--id <ID> (Optional)**

	The specified ID to access the shared file. **--pw <Password> (Optional)** The specified password to access the shared file. **--pw_file <Password File> (Optional)** The specified file path to read password. **--dev_id <Device ID> (Optional)** The specified device ID to manage specified device. The supported device ID: [1-3] Support [All] for action Unmount to unmount all devices. **--verify_cert (Optional)** Verify SSL certificate. (Only support for HTTPS protocol) **--accept_self_signed (Optional)** Accept self-signed certificate. (Only supported for HTTPS protocol)
VMShell	**--action <action>** Sets action to: 1 = devlist 2 = dev1drv 3 = dev1stop 4 = dev2iso 5 = dev2stop 6 = status 7 = log **--file <file name> (Optional)** Mounts the ISO image file for virtual media device 2. Use it with the dev2iso action. **--dev_id <Device ID> (Optional)** The specified device ID to get virtual media information. The supported device ID is [1-3]. Use it with the Status action. **--index <index> (Optional)** Mounts the drive with specified index for virtual media device 1. Use it with the dev1drv actions.

4.5.15. NM Management

NM Management	
Commands	**Long Options**

NmMeManage	**--type <type>** Manages Intel Management Engine with type: NM20 **--action <action>** Manages Intel Management Engine with action: GetDeviceID Reset ResetToDefault EnterToUpdateMode PowerOff SelfTest Mode ListImagesInfo GetPower GetTemp
GeneralNmManage	**--type <type>** Manages Intel Node Manager with a type: NM20 BMC10 **--action <action>** Manages Intel Node Manager with action: GetNMSDR GetSelTime GetStatistics ResetStatistics GetCapabilities GetVersion GetAlert SetAlert GetTotalPower SetTotalPower DelTotalPower SetPowerDrawRange GetSensor GetSummary **--mode <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 <Policy ID>** Applies for mode 11h or 12h. Otherwise, set to 0. **--domain_id <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 <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 **--value <assignment value>** Specifies SNMP sequence from 1 to 15. Checks SNMP sequence by SnmpManage command. **--range <Range>** Specifies power draw range. Power draw range: 0-32767 **--per_component_control <Per-component Control>** Allows for getting data for a chosen domain component. 0 - Accumulated data for whole domain will be returned. 1 - Data from single component in domain will be returned. **--component_id <Component ID>** Applies for mode 01h, 08h and per-component control = 1. Otherwise, set to 0. 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. 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. 3. For the PCIe Domain, the component identifier is the PCIe card index.

NmCpuManage	**--type <type>** Manages CPU with type: NM20 NM40 **--action <action>** Manages CPU with action: GetPState GetTState GetPTState GetCPUCores GetCPUMemTemp GetHostCPUData SetMaxAllowedPState SetMaxAllowedTState SetMaxAllowedCPUCores **--value <assignment value>** Specifies the maximum allowed CPU P-State. Checks number of P-State by GetPState action. **--socket <Socket number>** CPU socket number 0~7 - For which current settings should be read. 255 - All sockets will return common maximum settings. **--core <Core number>** Active cores configuration 255 - All sockets will return common maximum settings. **--limit <limit>** Turbo Ratio Limit 0 - Restore default settings. Others - Turbo Ratio Limit to set.
NmCupsManage	**--type <type>** Manages Compute Usage Per Second(CUPS) with type: NM30 **--action <action>** Manages Compute Usage Per Second(CUPS) with action: GetCUPSCapability GetCUPSData GetCUPSConfig GetCUPSPolicy GetCUPSCore GetCUPSIO GetCUPSMem SetCUPSPolicy

	EnableCUPSPolicy DisableCUPSPolicy **--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).
BmcNmManage	**--type <type>** Manages BMC Intel Manager with type: BMC10 **--action <action>** Manages Intel Management Engine with action: GetDeviceID GetPower GetTemp

4.5.16. Multi-Node Management

Multi-Node Management	
Commands	**Long Options**
GetTpInfo	**--file <file name> (Optional)** Saves the information to a file. Prints the TwinPro information on screen if the file-saving function is not available. **--overwrite (Optional)** Overwrites the output file.

ChangeTpInfo	**--file <file name>** Updates the TwinPro configuration with the given configuration file. **--individually (Optional)** Updates each TwinPro configuration with corresponding configuration file individually.
GetMultinodeEcInfo	**--file <file name> (Optional)** Reads the multi-node EC information from an input multi-node EC image file. **--file_only (Optional)** Works with the --file option, and only reads multi-node EC information from the input image file. **--json_view (Optional)** Sets the output format to JSON.
UpdateMultinodeEc	**--file <file name>** Updates the multi-node EC with the given multi-node EC image file. **--individually (Optional)** Updates each multi-node EC with corresponding FW file individually. **--force_update (Optional)** Ignores other nodes power status and forces to update.
GetMultinodeLcmcInfo	**--json_view (Optional)** Sets the output format to JSON.
UpdateMultinodeLcmc	**--file <file name>** Updates the multi-node LCMC with the given multi-node LCMC image file.

4.5.17. FPGA Management

FPGA Management	
Commands	**Long Options**
GetMotherboardFpgaInfo	**--file <file name> (Optional)** Reads the motherboard FPGA information from an input FPGA

	image file. **--file_only (Optional)** Works with the --file option, and only reads motherboard FPGA information from the input image file.
UpdateMotherboardFpga	**--file <file name>** Updates the motherboard FPGA with the given FW image file. **--reboot** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each motherboard FPGA with corresponding image file individually.

4.5.18. PCIe-Switch Management

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

	--post_complete (Optional) Waits for the managed system POST complete after rebooting.

4.5.19. Security Management

Security Management	
Commands	**Long Options**
BiosRotManage	**--action <action>** Sets action to: 1 = GetInfo 2 = UpdateGolden 3 = Recover 4 = DownloadEvidence **--file <file name> (Optional)** Works with --action DownloadEvidence. Saves the BIOS evidence to a file. **--overwrite (Optional)** Works with --action DownloadEvidence. Overwrites the output file. **--reboot (Optional)** Works with --action UpdateGolden and Recover. Forces the managed system to reboot or power up after operation. **--redfish (Optional)** Enables support for pure Redfish. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
BmcRotManage	**--action <action>** Sets action to: 1 = GetInfo 2 = UpdateGolden 3 = Recover 4 = DownloadEvidence **--file <file name> (Optional)** Works with --action DownloadEvidence. Saves the BMC evidence to a file. **--overwrite (Optional)** Works with --action DownloadEvidence. Overwrites the output file.

	--redfish (Optional) Enables support for pure Redfish.
CpldRotManage	**--action <action>** Sets action to: 1 = GetInfo 2 = UpdateGolden
SecureBootManage	**--action <action>** Sets action to: 1 = Status 2 = Enable 3 = Disable 4 = ShowDatabases 5 = UploadCertificate 6 = ResetAllKeysToDefault 7 = DeleteAllKeys 8 = DeletePK **--file <file name> (Optional)** Uploads secure boot key in the format of PEM. **--file_type <file type> (Optional)** Selects the type of secure boot key.The format of <file type> is "PK","KEK", "db", "dbr", "dbt" or "dbx" (case sensitive). Note that "dbx" can be only used with the "ShowDatabases" action **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--individually (Optional)** Updates each system secure boot keys individually with the corresponding secure boot key. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.
GetLockdownMode	**--json_view (Optional)** Sets the output format to JSON.
SetLockdownMode	**--lock <yes/no>** <yes/no> Locks/Unlocks the managed system. **--reboot (Optional)** Forces the managed system to reboot or power up after operation.

	--post_complete (Optional) Waits for the managed system's POST to complete after rebooting.
Attestation	**--action <action>** Sets action to: Dump List Download Delete GetInfo Compare **--file <file name> (Optional)** File name for measurement file. **--item <item name> (Optional)** Prints the specified item for the measurement file. (Only supported with the GetInfo action) **--overwrite (Optional)** Overwrites the downloaded or extracted file. **--showall (Optional)** Prints all information from the measurement file. (Only supported with the GetInfo action) **--file_only (Optional)** Gets information from the local measurement file. (Required option for the GetInfo action) **--nonce <nonce> (Optional)** Specify nonce for action Dump. **--ref <file name> (Optional)** Reference measurement file for comparison. (Only supported with the Compare action) **--root_cert <file name> (Optional)** Inputs the public certificate of Root CA to verify the certificate chain in measurement file. (Only supported with the GetInfo action) **--extract_certs <file name> (Optional)** Extracts endpoint certificate chain from the local measurement file. (Only supported with the GetInfo action) **--type <type> (Optional)** Specify dump type for action Dump. Supported types: MB

	--verify (Optional) Throw exception for file signature/certificate chain verification fail.
SecureEraseRaidHdd	**--json_view (Optional)** Sets the output format to JSON. **--dev_id <Device ID> (Optional)** A RAID controller ID for secure erase. **--enc_id <Enclosure ID> (Optional)** Enclosure ID list or "ALL" in the RAID controller for secure erase. **--dsk_id <Disk ID> (Optional)** Disk ID list or "ALL" in the RAID controller secure erase. **--tsk_id <Task ID> (Optional)** Accesses the progress of secure erase. **--abort (Optional)** Abort secure-erase operation. **--sync (Optional)** Shows the current progress of the secure-erase operation in RAID controller. **--precheck (Optional)** Shows the details of all disk ID list in the RAID controller. **--type <type> (Optional)** Vendor/Mode of RAID controller to do secure erase action: Broadcom IR mode = BRCM_IR Broadcom IT mode = BRCM_IT
SecureEraseDisk	**--file <file name>** HDD serial number mapping file. **--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--precheck (Optional)** Only displays HDD status. **--action <action> (Optional)** Sets secure erase action to:

	1 = SetPassword 2 = SecurityErase 3 = SecurityErasePWD 4 = SecurityErasePSID 5 = ChangePassword 6 = ClearPassword **--post_complete (Optional)** Waits for the managed system POST complete after rebooting. **--cur_pw_file <Current password file> (Optional)** The specified file path to read current password. **--json_view <-c SecureEraseDisk --file hddList.txt --precheck --json_view> (Optional)** Sets the output format to JSON.
TpmProvision	**--reboot** Forces the managed system to reboot or power up after operation. **--image_url <URL>** The URLs to access the shared image file. SAMBA URL: 'smb://<host name or IP>/<shared point>/<file path>' SAMBA UNC: '\<host name or IP><shared point><file path>' HTTP URL: 'http://<host name or IP>/<shared point>/<file path>' **--lock <yes/no>** <yes> Locks the TPM module. **--id <ID> (Optional)** The specified ID to access the shared file. **--pw <Password> (Optional)** The specified password to access the shared file. **--pw_file <Password File> (Optional)** The specified file path to read password. **--cleartpm (Optional)** Clears the ownership of the TPM module and restores the relevant TPM BIOS settings.
GetTpmInfo	**--current_password <current password> (Optional)** Checks the current BIOS Administrator password. **--showall (Optional)** Prints the NV data and the capability flags (if applicable) of the trusted platform module. (Only supported for Intel platform)

	--cur_pw_file <Current password file> (Optional) The specified file path to read current password.
TpmManage	**--reboot (Optional)** Forces the managed system to reboot or power up after operation. **--clear_and_enable_dtpm_txt (Optional)** Clears dTPM ownership and activates dTPM/TXT. **--clear_dtpm (Optional)** Clears dTPM ownership, and disables dTPM for TPM 1.2. Clears dTPM ownership for TPM 2.0 **--enable_txt_and_dtpm (Optional)** Enables TXT and dTPM. **--clear_and_enable_dtpm (Optional)** Clears dTPM ownership, disables dTPM (for TPM 1.2 only) and activates dTPM. **--disable_dtpm (Optional)** Disables dTPM. **--disable_txt (Optional)** Disables TXT. **--provision (Optional)** Launches the trusted platform module provision procedure. **--table_default (Optional)** Uses the default TPM provision table. **--table <table file> (Optional)** Uses the given customized TPM provision table file. **--post_complete (Optional)** Waits for the managed system’s POST to complete after rebooting.
GetCpuERotInfo	None

UpdateCpuERot	**--file <file name>** Updates the CPU ERoT with the given FW image file. **--individually (Optional)** Updates each CPU ERoT with corresponding configuration file individually.
CpuERotManage	**--action <action>** Sets action to: 1 = GetInfo 2 = UpdateGolden 3 = Recover
FpgaRotManage	**--action <action>** Sets action to: 1 = GetInfo 2 = UpdateGolden
GetGpuERotInfo	None
GetSpdmInfo	**--item <item name> (Optional)** Specify the item whose measurements and summary are to be displayed. **--showall (Optional)** Display all measurements and summary for the specified item.
CmmRotManage	**--action <action>** Sets action to: 1 = GetInfo 2 = UpdateGolden 3 = Recover 4 = DownloadEvidence **--file <file name> (Optional)** Works with the --action DownloadEvidence option and saves the CMM evidence to a file. **--overwrite (Optional)** Works with the --action DownloadEvidence option and overwrites the output file.

	--redfish (Optional) Enables pure Redfish support.
CertManage	**--action <action>** Sets action to: 0 = GetCertList 1 = GenerateCSR 2 = UploadCert 3 = DeleteCert **--cfg_file <Config file>** JSON file input need for generating the CSR token. **--file <file name> (Optional)** Output file for wring the CSR string or input file for reading the token content. **--type <type> (Optional)** The type of certificate needed for Uploading, Replacing, or Deleting the certificate. Supported types are: LDAP, CA, HTTP. **--certid <CERTIFICATE ID> (Optional)** Certificate ID that is needed for replacing the existing certificate or deleting the certificate.

4.5.20. MCU Management

MCU Management	
Commands	**Long Options**
GetMotherboardMcuInfo	**--json_view (Optional)** Sets the output format to JSON.
UpdateMotherboardMcu	**--file <file name>** Updates Motherboard MCU with the given image file. **--reboot** Forces the managed system to reboot or power up after operation. **--post_complete (Optional)** Waits for the managed system's POST to complete after reboot.

4.5.21. Switch Management

Switch Management	
Commands	**Long Options**
NvSwitchManage	**--action <action>** Sets action to: 1 = GetFwInfo 2 = UpdateFw 3 = GetNvosInfo 4 = ShowNvosSysImageList 5 = UpdateNvosSysImage **--file <file name> (Optional)** Firmware File to Update. **--comp <component id> (Optional)** The Component Id of the Nv Switch to Update or Get Information. **--reboot (Optional)** Flag to proceed for Rebooting the NV Switch after successful firmware update.
GetBladeSwitchInfo	**--file <file name> (Optional)** Reads the switch information from an input switch image file. **--dev_id <Device ID> (Optional)** Assigns switch index. Switch index: [A1,A2,B1,B2] or [ALL] **--file_only (Optional)** Works with --file, and only reads switch image information from the input image file. **--json_view (Optional)** Sets the output format to JSON.
UpdateBladeSwitch	**--file <file name>** Updates switch firmware with the given firmware file. **--switch_user <Switch user ID> (Optional)** Assigns switch user when updating through CMM. **--switch_pw <Switch user password> (Optional)** Assigns switch password when updating through CMM. **--reboot (Optional)**

	Forces the switch to reboot or power up after operation. **--individually (Optional)** Updates each switch module with corresponding firmware image individually. **--dev_id <Device ID> (Optional)** Assigns switch index when updating through CMM. Switch index: [A1,A2,B1,B2] or [ALL]
RebootBladeSwitch	**--dev_id <Device ID> (Optional)** Assigns switch index when rebooting via CMM. Switch index: [A1,A2,B1,B2] or [ALL] **--switch_user <Switch user ID> (Optional)** Assigns switch user when rebooting via CMM with switch credentials. **--switch_pw <Switch user password> (Optional)** Assigns switch password when rebooting via CMM with switch credentials.

4.5.22. Liquid Cooling Management

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

UpdateCDU	**--file <file name>** Updates CDU firmware with the given firmware bundle file. **--redfish (Optional)** Enables support for pure Redfish.

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	1. Defined by the option --journal_path. The log exists inside the “History” subfolder in the folder path defined by the option.--journal_path. 2. “/var/log/supermicro/SAA”. 3. $PWD in Linux or %cd% in Windows.
Critical error log	Always activated	1. Defined by the option --journal_path. The log exists inside the “Critical” subfolder in the folder path defined by the option. --journal_path. 2. /var/log/supermicro/SAA. 3. $PWD in Linux or %cd% in Windows.
Multiple system log	Always activated	1. Defined by the option --journal_path. The log exists inside the “Multiple” subfolder in the folder path defined by the option. --journal_path. 2. /var/log/supermicro/SAA.

		3. The same directory as multiple list file.
Command execution journal	Activated by configuration	1. Defined by the option --journal_path. The log exists in the folder path defined by the option. --journal_path. 2. Defined by .saarc in the home directory. 3. ~/journal/supermicro/saa/ in Linux or %HomePath%\journal\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>
```

- 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/MacAddr	/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/StaticIP	/BmcCfg/OemCfg/LAN/Configuration/IPv6/Co

v6/Configuration/IPv6StaticNameServer	nfiguration/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 “RAIDCfg.” <RAIDCfg> and </RAIDCfg> are its tag pair. All information in the root table is enclosed between this tag pair.
- There could be three child tags for the root table: “Information” and “BroadcomRAIDController” and “MarvellRAIDController.”
- “Information,” “BroadcomRAIDController” and “MarvellRAIDController” could have child tables.
- Configurable elements are listed in the “Configuration” field of each child table.
- Each configurable element has a tag pair. The element value is enclosed by its tag pair.

- Comments may be given following any element or table tag. Each comment is enclosed by the
- <!-” and “-->” tags. The supported usage of each element and table are shown in the comments that follow.
- Configuration tables may have “Action” attributes. Supported actions are shown in the comments. If the action is “None,” all configuration and child tables of this table will be skipped.
- Configuration tables may contain more table specific attributes when needed.

For Broadcom controller uses “BroadcomRAIDController” table:

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

For Marvell controller uses “MarvellRAIDController” table:

- To create a logical drive, the RAIDInfo action should be “Change” and the RAID action should be “Create.” The “ArrayID” field should be set to “0.”
- To delete a logical drive, the RAIDinfo action should be “Change”, the RAID action should be “Delete” and assigned the corresponding “LogicalDrive DriveID” to “LogicalDriveDeleteID.”

- To rebuild a logical drive, the RAIDinfo action should be “Change,” the RAID action should be “Rebuild” and assigned the corresponding “LogicalDrive DriveID” to “LogicalDriveRebuildID.”
- To import a logical drive, the RAIDinfo action should be “Change,” the RAID action should be “Import” and assigned the corresponding “LogicalDrive DriveID” to “LogicalDriveImportID.”



Notes:

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

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

- The number of physical hard drives must be a multiple of the "Span" value on the Broadcom controller.
- Marvell controller only supports RAID level 1.
- Marvell controller on AOC-SLG2-2TM2 supports up to two drives.

- For using tools to edit XML files, please refer to Appendix F. Using the Command Line Tool (XMLStarlet) to Edit XML Files.

```
<?xml version="1.0"?>
<RAIDCfg>
  <Information>
    <TotalRaidController>2</TotalRaidController>
  </Information>
  <BroadcomRAIDController Action="Change" DeviceID="0"
DeviceName="AVAGO 3108 MegaRAID">
    <!--Supported Action:None/Change-->
    <ControllerProperties Action="None">
      <!--Supported Action:None/Change-->
      <Configuration>
        <BiosBootMode>Stop on Error</BiosBootMode>
        <!--RAID controller BIOS boot mode, enumerated string
value-->
        <!--Supported values: Stop on Error/Pause on Error/Ignore
Errors/Safe Mode on Error-->
        <JbodMode>Disable</JbodMode>
        <!--RAID controller JBOD mode, enumerated string value-->
        <!--Supported values: Enable/Disable-->
      </Configuration>
    </ControllerProperties>
    <RAIDInfo Action="Change">
      <!--Supported Action:None/Change/ClearAll-->
      <RAID Action="None" ArrayID="-1">
        <!--Supported
Action:None/Add/Delete/Create/Locate/Unlocate-->
        <Information>
          <PhysicalDriveCount>0</PhysicalDriveCount>
          <!--Total number of physical drives in this RAID-->
          <LogicalDriveCount>0</LogicalDriveCount>
          <!--Total number of logical drives in this RAID-->
          <LocatedPhysicalDriveList></LocatedPhysicalDriveList>
          <!--located physical drives-->
          <FreeSize>0</FreeSize>
          <!--Free size of RAID, unit: MB-->
          <LogicalDriveInfo></LogicalDriveInfo>
        </Information>
        <Configuration>
          <!--For each field, default support Create/Add actions if
not specially commented-->
          <Level>RAID0</Level>
          <!--RAID level, enumerated string value-->
          <!--Supported values:
RAID0/RAID1/RAID5/RAID6/RAID10/RAID50/RAID60-->
          <!--Only used for "Create" action-->
          <Span>1</Span>
          <!--PD span value, integer value-->
          <!--For RAID 0/1/5/6, valid value is 1-->
          <!--For RAID 10, valid value is 2 or 4-->
```

```
          <!--For RAID 50/60, valid value is 3 or 4-->
          <!--Only used for "Create" action-->
          <PhysicalDriveList></PhysicalDriveList>
          <!--Number of physical hard drive must be multiple of
"Span" value-->
          <!--Physical drive ID list of this RAID, integer values
separated by comma.-->
          <!--Can not use physical hard drive which present in
other RAID.-->
          <!--Can not use "Error" status physical HDD.-->
          <!--Can not use repeated physical hard drive ID in same
RAID.-->
          <!--Physical hard drive ID can not use negative number.--
>
          <!--Physical hard drive count can't be more than 32.-->
          <!--For RAID0, minimum number of physical HDD is 1.-->
          <!--For RAID1, minimum number of physical HDD is 2.-->
          <!--For RAID5, minimum number of physical HDD is 3.-->
          <!--For RAID6, minimum number of physical HDD is 3.-->
          <!--For RAID10, minimum number of physical HDD is 4.-->
          <!--For RAID50, minimum number of physical HDD is 6.-->
          <!--For RAID60, minimum number of physical HDD is 6.-->
          <!--Only used for "Create" action.-->
          <NewLogicalCount>1</NewLogicalCount>
          <!--Number of new Logical drive to be created/added-->
          <!--Integer value, valid value from 1 to 16-->
          <!--Can not run "Add" action when RAID has no any
physical hard drive.-->
          <!--Only used for "Create" and "Add" action-->
          <PercentageToUsed>100</PercentageToUsed>
          <!--Percentage to use, integer value between 1 and 100.--
>
          <!--Only used for "Create" and "Add" action-->
          <StripSize>256KB</StripSize>
          <!--Strip size of each logical drive-->
          <!--Enumerated integer value, unit is Byte-->
          <!--Valid value: 64KB/128KB/256KB/512KB/1MB-->
          <!--Default value: 256KB-->
          <!--Only used for "Create" and "Add" action-->
          <LogicalDriveName></LogicalDriveName>
          <!--Name of logical drive, string value-->
          <!--Maximum length: 15, empty string is accepted-->
          <!--Only used for "Create" and "Add" action-->
          <LogicalDriveReadPolicy>No Read
Ahead</LogicalDriveReadPolicy>
          <!--Read policy of logical drive, enumerated string
value-->
          <!--Possible values: No Read Ahead/Always Read Ahead-->
          <!--Default value: No Read Ahead-->
          <!--The value in this field does not indicate current
setting, it is the reference value for configuring purpose only-->
          <!--Only used for "Create" and "Add" action-->
          <LogicalDriveWritePolicy>Write
```

```
Back</LogicalDriveWritePolicy>
          <!--Write policy of logical drive, enumerated string
value-->
          <!--Possible values: Write Through/Write Back/Write Back
With BBU-->
          <!--Default value: Write Back-->
          <!--The value in this field does not indicate current
setting, it is the reference value for configuring purpose only-->
          <!--Only used for "Create" and "Add" action-->
          <LogicalDriveIoPolicy>Direct IO</LogicalDriveIoPolicy>
          <!--IO policy of logical drive, enumerated string value--
>
          <!--Possible values: Direct IO/Cached IO-->
          <!--Default value: Direct IO-->
          <!--The value in this field does not indicate current
setting, it is the reference value for configuring purpose only-->
          <!--Only used for "Create" and "Add" action-->
          <AccessPolicy>Read Write</AccessPolicy>
          <!--Access policy of logical drive, enumerated string
value-->
          <!--Possible values: Read Write/Read Only/Blocked-->
          <!--Default value: Read Write-->
          <!--The value in this field does not indicate current
setting, it is the reference value for configuring purpose only-->
          <!--Only used for "Create" and "Add" action-->
          <DiskCachePolicy>UnChanged</DiskCachePolicy>
          <!--Cache policy of logical drive, enumerated string
value-->
          <!--Possible values: UnChanged/Enable/Disable-->
          <!--Default value: UnChanged-->
          <!--The value in this field does not indicate current
setting, it is the reference value for configuring purpose only-->
          <!--Only used for "Create" and "Add" action-->
          <InitState>No Init</InitState>
          <!--Initial state of logical drive, enumerated string
value-->
          <!--Possible values: No Init/Quick Init/Full Init-->
          <!--Default value: No Init-->
          <!--The value in this field does not indicate current
setting, it is the reference value for configuring purpose only-->
          <!--Only used for "Create" and "Add" action-->
          <DeletingLogicalDriveList></DeletingLogicalDriveList>
          <!--Logical drive ID list for deleting, integer values
separated by comma-->
          <!--Logical drive for deleting can not use negative
number-->
          <!--Logical drive for deleting should be physical hard
drive of this RAID-->
          <!--Can not use repeated physical hard drive ID in same
RAID.-->
          <!--All logical physical hard drives of RAID will be
deleted when fill "ALL"-->
          <!--Can not run "Delete" action when RAID has no any
```

```
physical hard drive.-->
          <!--Only used for "Delete" action.-->
          <LocatingPhysicalDriveIDList>
</LocatingPhysicalDriveIDList>
          <!--Physical drive ID list for locating: integer values
separated by comma-->
          <!--Physical drive for locating can not use negative
number-->
          <!--Physical drive for locating should be physical hard
drive of this RAID-->
          <!--All physical hard drives of RAID will be located when
fill "ALL"-->
          <!--Can not use repeated physical hard drive ID in same
RAID.-->
          <!--Can not run "Locate" action when RAID has no any
physical hard drive.-->
          <!--Only used for "Locate" action-->
          <UnlocatePhysicalDriveIDList>
</UnlocatePhysicalDriveIDList>
          <!--Physical drive ID list for unlocating: integer values
separated by comma-->
          <!--Physical drive for unlocating can not use negative
number-->
          <!--Physical drive for unlocating should be physical hard
drive of this RAID-->
          <!--All physical hard drives of RAID will be unlocated
when fill "ALL"-->
          <!--Can not use repeated physical hard drive ID in same
RAID.-->
          <!--Can not run "Unlocate" action when RAID has no any
physical hard drive.-->
          <!--Only used for "Unlocate" action-->
        </Configuration>
      </RAID>
    </RAIDInfo>
  </RAIDController>
  <MarvellRAIDController Action="Change" DeviceID="0">
    <!--Supported Action:None/Change-->
    <ControllerProperties>
      <Information>
        <Controller>Marvell</Controller>
        <!--RAID controller-->
        <ControllerName>MRVL Storage System</ControllerName>
        <!--RAID controller name-->
        <ControllerSpeed>5.0 GT/s</ControllerSpeed>
        <!--RAID controller speed-->
        <ControllerStatus>OK</ControllerStatus>
        <!--RAID controller status-->
        <ChipRevision>a1</ChipRevision>
        <!--RAID controller chip revision-->
        <ControllerPCIeLinkWidth>2x Width</ControllerPCIeLinkWidth>
        <!--RAID controller PCIe link width-->
        <RomVersion>0.0.21.1005</RomVersion>
```

```
        <!--RAID controller rom version-->
        <LoaderVersion>2.1.0.1009</LoaderVersion>
        <!--RAID controller loader version-->
        <LegacyBIOSVersion>1.0.0.1031</LegacyBIOSVersion>
        <!--RAID controller legacy BIOS version-->
        <UEFIAHCIDriverVersion>1.1.21.1002</UEFIAHCIDriverVersion>
        <!--RAID controller UEFI AHCI driver version-->
        <I2CProtocolVersion>0.0.0.20</I2CProtocolVersion>
        <!--RAID controller I2C protocol version-->
        <PN></PN>
        <!--RAID controller PN-->
        <AOCVersion></AOCVersion>
        <!--RAID controller AOC version-->
        <SerialNumber></SerialNumber>
        <!--RAID controller serial number-->
        <FirmwareVersion></FirmwareVersion>
        <!--RAID controller firmware version-->
        <Batch></Batch>
        <!--RAID controller batch-->
      </Information>
    </ControllerProperties>
    <PhysicalDriveInfo>
      <Information>
        <!--Physical hard drive information, this region is read
only.-->
        <DriveCount>2</DriveCount>
        <PhysicalDrive DriveID="0">
          <EnclosureID>0</EnclosureID>
          <!--Enclosure ID, string value-->
          <DriveStatus>OK</DriveStatus>
          <!--Physical drive alive status, enumerated string value-
->
          <!--Possible values: OK/Warning-->
          <Temperature>46</Temperature>
          <!--Physical drive temperature in degree C, integer
value-->
          <Capacity>480</Capacity>
          <!--Physical drive capacity in Gigabyte, integer value-->
          <ModelName>Micron_5300_MTFDDAV480TDS</ModelName>
          <!--Physical drive model name, string value-->
          <Revision> D3MU001</Revision>
          <!--Physical drive firmware revision, string value-->
          <SerialNumber>ABCDE</SerialNumber>
          <!--Physical drive serial number, string value-->
          <LinkSpeed>6</LinkSpeed>
          <!--Physical drive link speed value, string values-->
          <!--Unit is Gb/s-->
          <FirmwareConfiguredState>OK</FirmwareConfiguredState>
          <!--Firmware status of physical drive.-->
          <PredictedFail>false</PredictedFail>
          <!--Physical drive predicted fail-->
          <!--Possible values: true/false-->
        </PhysicalDrive>
```

```
        <PhysicalDrive DriveID="1">
          <EnclosureID>1</EnclosureID>
          <!--Enclosure ID, string value-->
          <DriveStatus>OK</DriveStatus>
          <!--Physical drive alive status, enumerated string value-
->
          <!--Possible values: OK/Warning-->
          <Temperature>47</Temperature>
          <!--Physical drive temperature in degree C, integer
value-->
          <Capacity>480</Capacity>
          <!--Physical drive capacity in Gigabyte, integer value-->
          <ModelName>Micron_5300_MTFDDAV480TDS</ModelName>
          <!--Physical drive model name, string value-->
          <Revision> D3MU001</Revision>
          <!--Physical drive firmware revision, string value-->
          <SerialNumber>ABCDE</SerialNumber>
          <!--Physical drive serial number, string value-->
          <LinkSpeed>6</LinkSpeed>
          <!--Physical drive link speed value, string values-->
          <!--Unit is Gb/s-->
          <FirmwareConfiguredState>OK</FirmwareConfiguredState>
          <!--Firmware status of physical drive.-->
          <PredictedFail>false</PredictedFail>
          <!--Physical drive predicted fail-->
          <!--Possible values: true/false-->
        </PhysicalDrive>
      </Information>
    </PhysicalDriveInfo>
    <RAIDInfo Action="Change">
      <!--Supported Action:None/Change-->
      <RAID Action="None" ArrayID="0">
        <!--Supported Action:None/Delete/Create/Rebuild/Import-->
        <Information>
          <PhysicalDriveCount>2</PhysicalDriveCount>
          <!--Total number of physical drives in this RAID-->
          <LogicalDriveCount>1</LogicalDriveCount>
          <!--Total number of logical drives in this RAID-->
          <LogicalDrive DriveID="0">
            <DriveStatus>OK</DriveStatus>
            <!--Logical drive alive status-->
            <!--Possible values: OK/Warning-->
            <Capacity>447</Capacity>
            <!--Logical drive capacity, integer value-->
            <!--Unit is GB-->
            <RaidLevelQualifier>RAID1</RaidLevelQualifier>
            <!--RAID level qualifier of logical drive, enumerated
value-->
            <!--Possible values: RAID1-->
            <LDStripSize>64K</LDStripSize>
            <!--Strip size of logical drive, enumerated value-->
            <!--Unit is Byte-->
            <!--Possible values: 32K/64K-->
```

```
            <PD0Registered>Yes</PD0Registered>
            <!--Physical drive #0 registered-->
            <!--Possible values: Yes/No-->
            <PD1Registered>Yes</PD1Registered>
            <!--Physical drive #1 registered-->
            <!--Possible values: Yes/No-->
            <FirmwareState>Optimal</FirmwareState>
            <!--Firmware state for this RAID, enumerated string
value-->
            <!--Possible values:
Offline/Foreign/Degraded/Rebuilding/Optimal-->
            <Name>SuperFuck</Name>
            <!--Name of logical drive, string value-->
          </LogicalDrive>
        </Information>
        <Configuration>
          <!--For each field, default support Create actions if not
specially commented-->
          <Level>RAID1</Level>
          <!--RAID level, enumerated string value-->
          <!--Only supported value: RAID1-->
          <!--Only used for "Create" action-->
          <StripSize>32K</StripSize>
          <!--Strip size of each logical drive-->
          <!--Enumerated integer value, unit is Byte-->
          <!--Valid value: 32K/64K-->
          <!--Default value: 64K-->
          <!--Only used for "Create" action-->
          <LogicalDriveName><![CDATA[]]></LogicalDriveName>
          <!--Name of logical drive, string value-->
          <!--Maximum length: 15-->
          <!--Should not contains space and double quote-->
          <!--Only used for "Create" action-->
          <LogicalDriveDeleteID>0</LogicalDriveDeleteID>
          <!--Delete virtual drive ID, integer value-->
          <!--ID number should be LogicalDrive DriveID-->
          <!--Should not set bigger than LogicalDrive DriveID-->
          <!--Only used for "Delete" action-->
          <LogicalDriveImportID>0</LogicalDriveImportID>
          <!--Import virtual drive ID, integer value-->
          <!--ID number should be LogicalDrive DriveID-->
          <!--Should not set bigger than LogicalDrive DriveID-->
          <!--Only used for "Import" action-->
          <LogicalDriveRebuildID>0</LogicalDriveRebuildID>
          <!--Rebuild virtual drive ID, integer value-->
          <!--ID number should be LogicalDrive DriveID-->
          <!--Should not set bigger than LogicalDrive DriveID-->
          <!--Only used for "Rebuild" action-->
        </Configuration>
      </RAID>
    </RAIDInfo>
  </Marvell9230RAIDController>
```

```
</RAIDCfg>
```

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.

```
<?xml version="1.0"?>
<VROCCfg>
  <!--SuperServer Automation Assistant 1.3.0_alpha (2025/01/16)-->
  <!--File generated at 2025-02-03_14:43:51-->
  <PhysicalDriveInfo>
    <Information>
      <!--Physical hard drive information, this region is read only.-->
      <DriveCount>2</DriveCount>
      <PhysicalDrive VROCId="25362e54-a291-5a0f-a3e7-71ec761b4838">
        <!--This VROCId is used to identify drive-->
        <DriveStatus>Enabled</DriveStatus>
        <!--Physical drive status, string value-->
        <Temperature>0</Temperature>
        <!--Physical drive temperature in degree C, integer value-->
        <Capacity>2980</Capacity>
        <!--Physical drive capacity in Gigabyte, integer value-->
        <ModelName>INTEL SSDPE2KE032T8</ModelName>
        <!--Physical drive model name, string value-->
        <SerialNumber>PHLN1175029U3P2BGN</SerialNumber>
        <!--Physical drive serial number, string value-->
        <CapableSpeed>0Gb/s</CapableSpeed>
        <!--Physical drive capable speed value, string value-->
        <PredictedFail>false</PredictedFail>
        <!--Physical drive predicted fail, string value-->
      </PhysicalDrive>
      <PhysicalDrive VROCId="bd46b207-9de2-5291-b80a-562d7170f0de">
        <!--This VROCId is used to identify drive-->
        <DriveStatus>Enabled</DriveStatus>
        <!--Physical drive status, string value-->
        <Temperature>0</Temperature>
        <!--Physical drive temperature in degree C, integer value-->
        <Capacity>2980</Capacity>
        <!--Physical drive capacity in Gigabyte, integer value-->
        <ModelName>INTEL SSDPE2KE032T8</ModelName>
        <!--Physical drive model name, string value-->
        <SerialNumber>PHLN117500TA3P2BGN</SerialNumber>
        <!--Physical drive serial number, string value-->
```

```
        <CapableSpeed>0Gb/s</CapableSpeed>
        <!--Physical drive capable speed value, string value-->
        <PredictedFail>false</PredictedFail>
        <!--Physical drive predicted fail, string value-->
      </PhysicalDrive>
    </Information>
  </PhysicalDriveInfo>
  <VolumeInfo Action="Change">
    <!--Supported Action:None/Change/ClearAll-->
    <Volume Action="None" VROCId="e66e93dc-a28b-5072-8c02-ec48ecb3bccb">
      <!--Supported Action:None/Delete/Create-->
      <!--This VROCId is used to identify volume-->
      <Information>
        <Encrypted>false</Encrypted>
        <!--Encryption status of this volume-->
        <BlockSize>512</BlockSize>
        <!--Block size (Bytes), integer value-->
      </Information>
      <Configuration>
        <Name>TestRaid_0</Name>
        <!--Volume name, string value; length limit = 15 characters-->
        <!--Only used for "Create" action-->
        <Level>RAID1</Level>
        <!--RAID level, string value-->
        <!--Valid value: RAID0/RAID1/RAID5/RAID10-->
        <!--Only used for "Create" action-->
        <PhysicalDriveList></PhysicalDriveList>
        <!--Physical drive list, string value-->
        <!--Use commas to separate-->
        <!--Support VROCId and Serial Number-->
        <!--Valid drive count:-->
        <!--1~96, Any number for RAID0-->
        <!--2~2, Even number for RAID1-->
        <!--3~96, Any number for RAID5-->
        <!--4~4, Even number for RAID10-->
        <!--Only used for "Create" action-->
        <StripSize>64</StripSize>
        <!--Strip size (KB), integer value-->
        <!--Valid value: -->
        <!--4/8/16/32/64/128 for RAID0-->
        <!--64 for RAID1-->
        <!--4/8/16/32/64/128 for RAID5-->
        <!--4/8/16/32/64/128 for RAID10-->
        <!--Only used for "Create" action-->
        <Capacity>2899742</Capacity>
        <!--Capacity size (MB), integer value-->
        <!--Only used for "Create" action-->
      </Configuration>
    </Volume>
  </VolumeInfo>
</VROCCfg>
```

- 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-->
        <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:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI Hard Disk:UEFI OS (SATA,Port:0)</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #2" selectedOption="UEFI CD/DVD" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI CD/DVD</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #3" selectedOption="UEFI USB Hard Disk"
type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB Hard Disk</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #4" selectedOption="UEFI USB CD/DVD"
type="Option">
```

```
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB CD/DVD</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #5" selectedOption="UEFI USB Key" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB Key</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #6" selectedOption="UEFI USB Floppy"
type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB Floppy</DefaultOption>
      </Information>
```

```
    </Setting>
    <Setting name="Boot Option #7" selectedOption="UEFI USB Lan" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI USB Lan</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #8" selectedOption="UEFI Network:(B4/D0/F0) UEFI
PXE IPv4 Intel® Ethernet Controller X550(MAC:3cecefcb33c6)" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</DefaultOption>
      </Information>
    </Setting>
    <Setting name="Boot Option #9" selectedOption="UEFI Hard Disk:UEFI OS
(SATA,Port:0)" type="Option">
      <Information>
        <AvailableOptions>
          <Option>UEFI Hard Disk:UEFI OS (SATA,Port:0)</Option>
          <Option>UEFI CD/DVD</Option>
          <Option>UEFI USB Hard Disk</Option>
          <Option>UEFI USB CD/DVD</Option>
          <Option>UEFI USB Key</Option>
          <Option>UEFI USB Floppy</Option>
          <Option>UEFI USB Lan</Option>
          <Option>UEFI Network:(B4/D0/F0) UEFI PXE IPv4 Intel® Ethernet
Controller X550(MAC:3cecefcb33c6)</Option>
          <Option>UEFI AP:UEFI: Built-in EFI Shell</Option>
```

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

```
          <Option>Disabled</Option>
        </AvailableOptions>
        <DefaultOption>(B4/D0/F1) UEFI PXE IPv4 Intel® Ethernet Controller
X550(MAC:3cecefcb33c7)</DefaultOption>
      </Information>
    </Setting>
  </Menu>
</FixedBootCfg>
```

- The XML version is shown in the first line.
- The root table name is "*FixedBootCfg.*" Its name tag pair is <*FixedBootCfg*> and *</FixedBootCfg>*. All information belonging to the root table is enclosed between this name tag pair.
- There could be several menus in FixedBootCfg, depending on your managed system's boot device.
- Configurable elements are listed in the "<*Setting*>" field of each child table.
- Each name tag pair <*Menu*> encloses name tag pairs <*Menu*>, <*Information*>, <*Setting*>.
- <*Information*> shows the setting-specific information. For example, <*Setting*> with the attribute "name" as "Option" has <*AvailableOptions*> and <*DefaultOption*> to indicate the selectable and default options, respectively. Any modification in the* <Information>*enclosure is unnecessary and NEVER takes effect.
- Change setting you can modify after # number or change selectedOption <*Setting name="UEFINetwork #2" selectedOption="(B4/D0/F0)UEFI PXE IPv4 Intel® Ethernet Controller X550(MAC:3cecefcb33c6)" type="Option"*>
- Comments could be given to the following element or table name tag. Each comment is enclosed by "<!--" and "-->" tags.

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

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



Notes:

- Unchanged settings can be deleted to skip the update.

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

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.



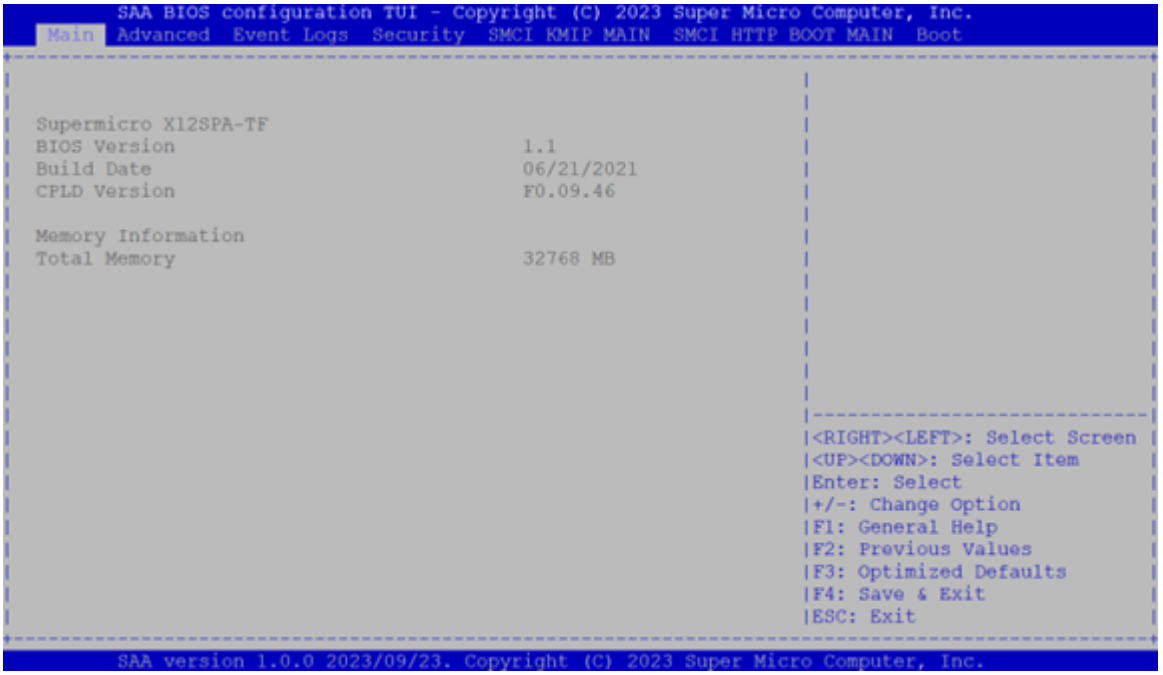
Notes:

- 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

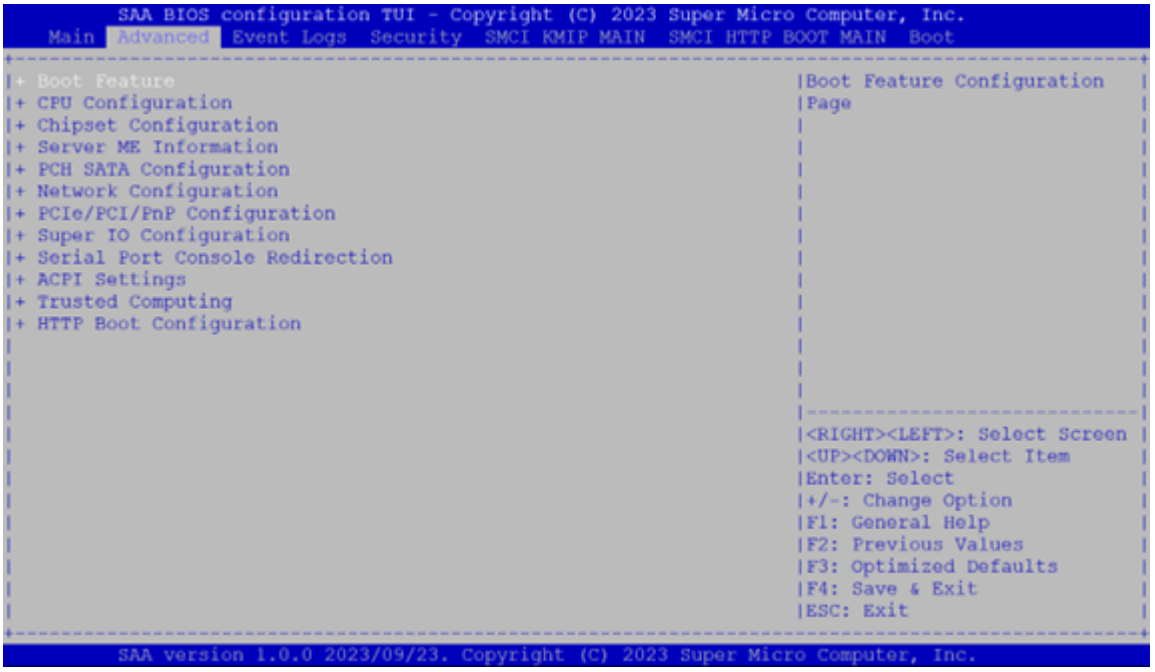
- **Using Arrow Keys**

  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.



- **Setting Values**

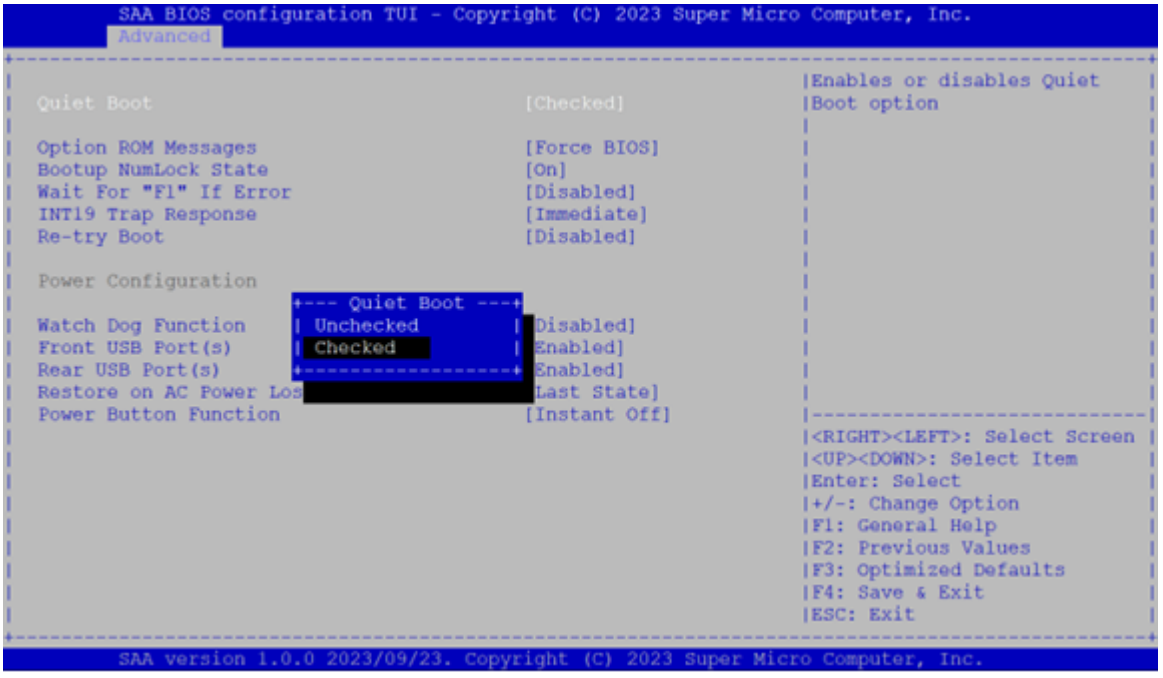
  A “+” symbol before an option on a menu indicates that a sub-menu can be expanded for further configuration. To change a setting value, you can press the keys **<+>** and **<->**. Or you can press the **<Enter>** key to call up a dialog box for configuration.



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

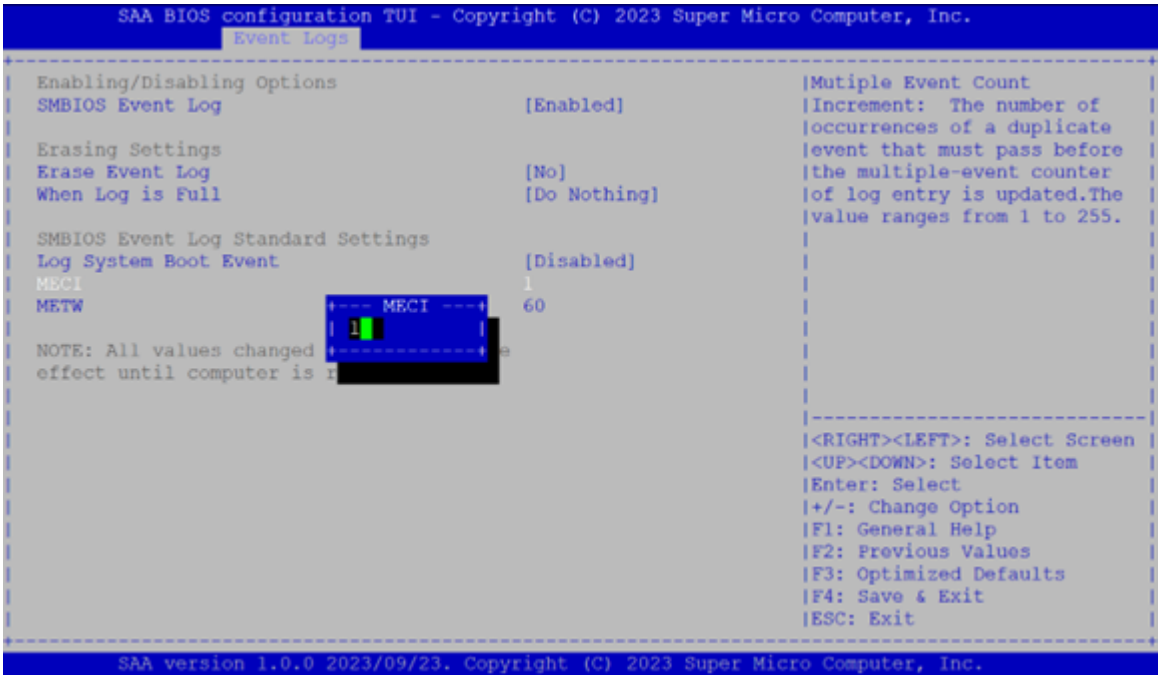
  Some functions are allowed to be enabled or disabled. To change the setting, press the **<Enter>** key to call up a dialog box. Press the **<UP>** and **<DOWN>** arrow keys

to make a selection. To disable a function, select **Unchecked**. To enable a function, select **Checked**.



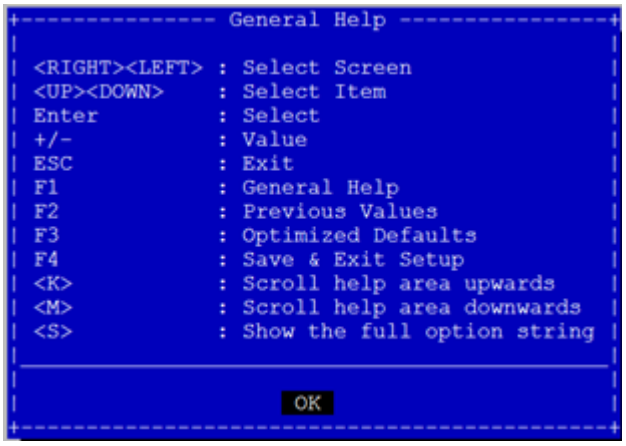
- **Setting Numeric Values**

  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.



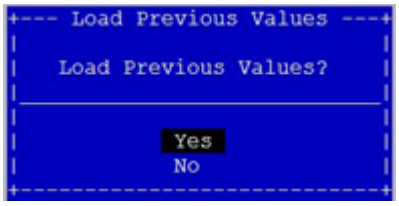
4.9.2.3. Getting General Help

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



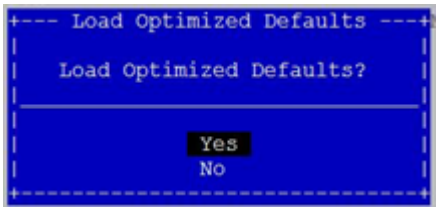
4.9.2.4. Loading Previous Values

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



4.9.2.5. Loading Optimized Values

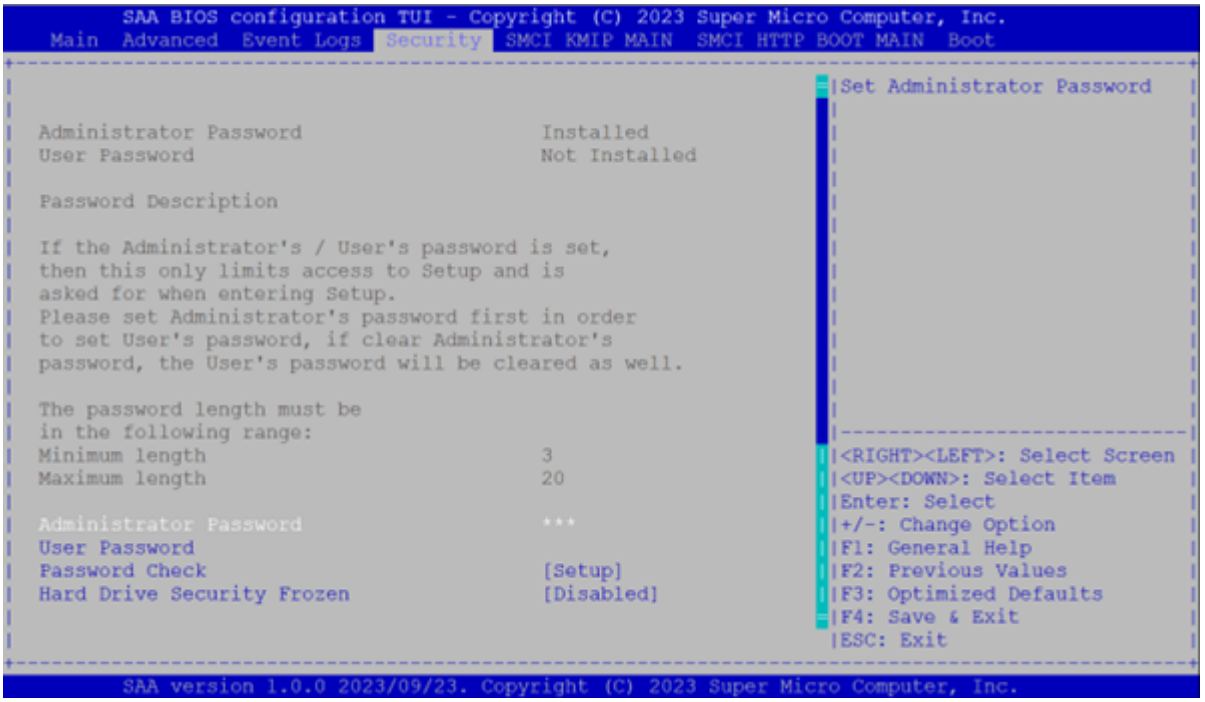
To return all configurations to the default values, press the **<F3>** key. A message appears for confirmation.



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:

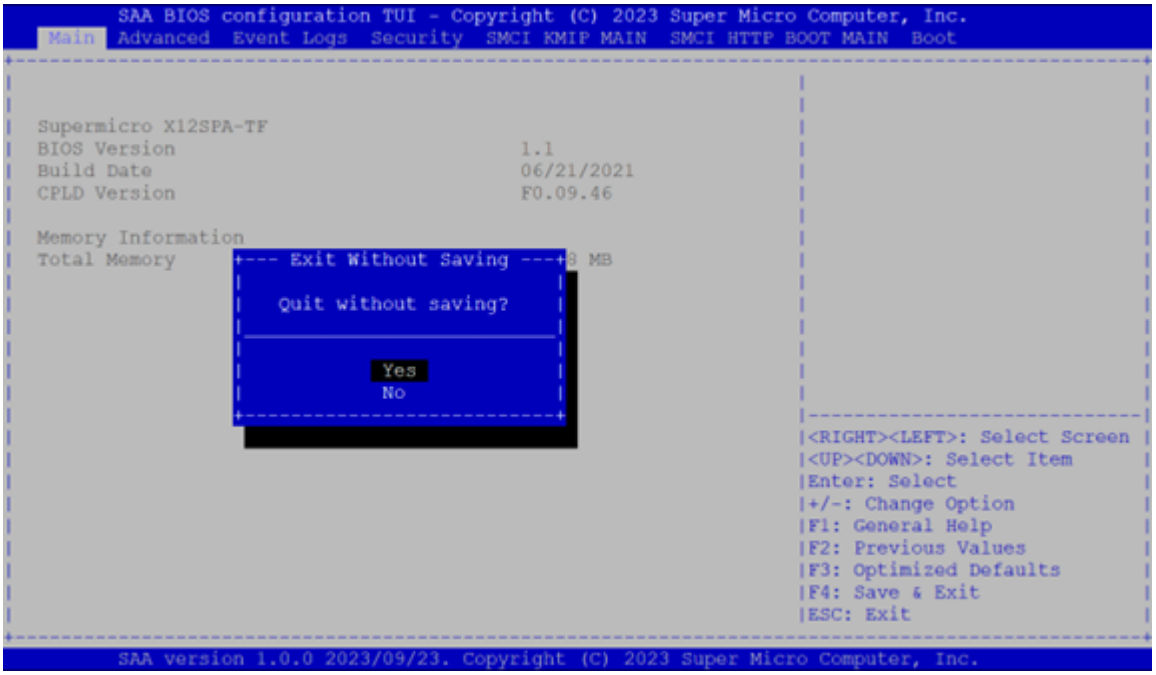
- If you have already set passwords in your BIOS, a series of three asterisks on the Security page indicates that a password is created (see the figure below).
- The password length may vary depending on the BIOS you use. For example, the length of the password can be from 3 to 20 characters long (see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



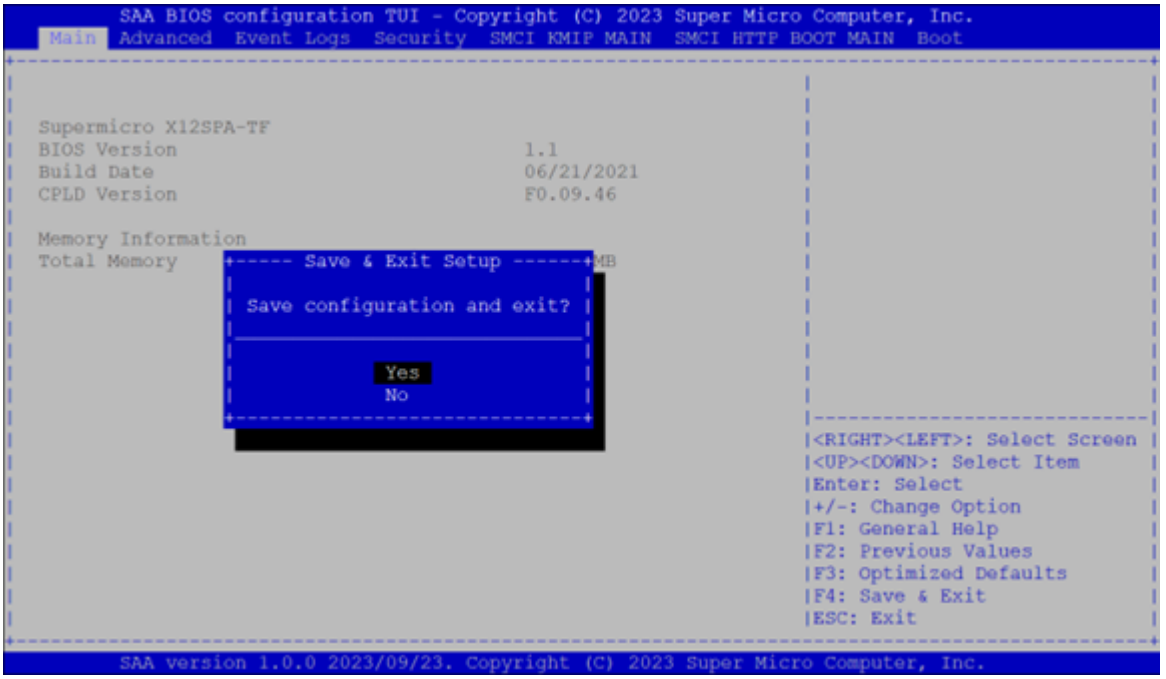
4.9.2.7. Exiting the TUI

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.



4.10. JSON View

The --json_view option displays output in **JSON format only**. When enabled, no banner, progress threads, warnings, or extra messages are shown—only the JSON result.

Supported commands JSON schema and their JSON sample files can be found in the json_schema folder.

Supported Commands

CheckOOBSupport	CheckSensorData	GetFruInfo
CheckAssetInfo	GetSystemInfo	GetFirmwareInventoryInfo
GetBiosInfo	GetDmiInfo	GetScpInfo
GetBootOption	GetBmcInfo	GetKcsPriv
GetBmcUserList	GetLockdownMode	GetSessionInfo
BmcHostName	GetEventLog	GetMaintenEventLog
GetHostDump	GetCmmInfo	GetBbpInfo
GetBladePowerStatus	GetBladeSwitchInfo	BladePsuManage
GetFanMode	BladeSummary	GetCmmUserList
GetRaidControllerInfo	GetSataInfo	GetNvmeInfo
GetPMemInfo	GetSmartData	GetSasExpanderInfo
GetPsuInfo	GetPowerStatus	QueryProductKey
DCMIManage	GetCpldInfo	GetBackplaneCpldInfo
LocateServerUid	MonitorCDUStatus	MemoryHealthCheck
SystemPFA	PowerPolicy	SecureEraseDisk

SecureEraseRaidHdd	GetGpuInfo	NVSwitchManage

Examples

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


```
{
  "metadata": {
    "application_name": "SuperServer Automation Assistant",
    "version": "1.4.0",
    "build_date": "2025/06/25",
    "architecture": "x86_64",
    "schema_version": "saa-v1.0.0-GetBmcInfo-v1.0.0",
    "command": "./saa -c getbmcinfo --json_view",
    "managed_system": "localhost"
  },
  "data": [
    {
      "data_type": "GetBmcInfo.ManagedSystem",
      "bmc_type": "X12_RoT_ATEN_AST2500",
      "version": "01.05.07",
      "ext_version": "01 00 00 (P)",
      "build_date": "2024-11-22"
    }
  ]
}
```


```
[SAA_HOME]# ./saa -c GetGpuINFO --json_view
```


```
{
  "metadata": {
    "application_name": "SuperServer Automation Assistant",
    "version": "1.4.0",
    "build_date": "2025/06/25",
    "architecture": "x86_64",
    "schema_version": "saa-v1.0.0-GetGpuInfo-v1.0.0",
    "command": "./saa -c GetGpuInfo --json_view ",
    "managed_system": "localhost"
  },
  "error": {
    "exit_code": 11,
    "description": "Invalid command line data",
```

```
    "program_error_code": "47.92",
    "error_message": [
      "Invalid command line parameters. GetGpuInfo does not support --json_view
option."
    ],
    "instruction": [],
    "error_type": "ERROR",
    "chained_errors": []
  }
}
```


Multi OOB Example

```
[SAA_HOME]# ./saa -c GetBmcInfo -l ip.txt --json_view
```


```
{
  "metadata": {
    "application_name": "SuperServer Automation Assistant",
    "version": "1.4.0",
    "build_date": "2025/07/02",
    "architecture": "x86_64",
    "schema_version": "saa-v1.0.0-MultiOOB-INBAND-v1.0",
    "command": "./saa -c GetBmcInfo --json_view  -l ip.txt"
  },
  "summary": {
    "executions": 2,
    "waiting": 0,
    "running": 0,
    "success": 2,
    "failed": 0,
    "incomplete": 0,
    "retry": 0,
    "ignored": 0,
    "cancel": 0,
    "status_list": [
      {
        "elapsed": "00:00:00",
        "end_time": "07-16_00:57:56",
        "exit_code": 0,
        "index": 1,
        "start_time": "07-16_00:57:56",
        "status": "SUCCESS",
        "system_name": "10.184.21.146"
      },
      {
        "elapsed": "00:00:01",
        "end_time": "07-16_00:57:57",
```

```
        "exit_code": 0,
        "index": 2,
        "start_time": "07-16_00:57:56",
        "status": "SUCCESS",
        "system_name": "10.184.28.71"
      }
    ]
  },
  "data": [
    {
      "metadata": {
        "application_name": "SuperServer Automation Assistant",
        "version": "1.4.0",
        "build_date": "2025/07/02",
        "architecture": "x86_64",
        "schema_version": "saa-v1.0.0-GetBmcInfo-v1.0.0",
        "command": "",
        "managed_system": "10.184.21.146"
      },
      "data": [
        {
          "data_type": "GetBmcInfo.ManagedSystem",
          "uffn": "BMC_X13AST2600-F201MS_20240131_01.02.00_STDsp.bin",
          "bmc_type": "X12_ATEN_AST2600_1_1",
          "version": "01.02.00",
          "build_date": "2024/01/31"
        }
      ]
    },
    {
      "metadata": {
        "application_name": "SuperServer Automation Assistant",
        "version": "1.4.0",
        "build_date": "2025/07/02",
        "architecture": "x86_64",
        "schema_version": "saa-v1.0.0-GetBmcInfo-v1.0.0",
        "command": "",
        "managed_system": "10.184.28.71"
      },
      "data": [
        {
          "data_type": "GetBmcInfo.ManagedSystem",
          "uffn": "BMC_X14AST2600-C601MS_20250307_01.01.05.00_STDsp.bin",
          "bmc_type": "X14_OpenBMC_AST2600_1_1",
          "version": "01.01.05.00",
          "build_date": "2025/03/07"
        }
      ]
    }
  ]
}
```

Schema


```
{
  "metadata": {
    "application_name": "String",
    "version": "String",
    "build_date": "String",
    "architecture": "String",
    "command": "String",
    "schema_version": "String",
    "managed_system": "String"
  },
  "summary": {
    "executions": "Number",
    "waiting": "Number",
    "running": "Number",
    "success": "Number",
    "failed": "Number",
    "incomplete": "Number",
    "retry": "Number",
    "ignored": "Number",
    "cancel": "Number",
    "status_list": [
      {
        "elapsed": "String",
        "end_time": "String",
        "exit_code": "Number",
        "index": "Number",
        "start_time": "String",
        "status": "String",
        "system_name": "String"
      }
    ]
  },
  "data": [
    {
      "data_type": "String"
    }
  ],
  "messages": [
    {
      "timestamp": "String",
      "severity": "String",
      "message": "String"
    }
  ],
  "error": {
    "exit_code": 0,
    "description": "String",
    "program_error_code": "String",
    "error_message": [
      "String"
```

```
    ],
    "instruction": [
      "String"
    ]
  }
}
```

Field Descriptions

metadata: Contextual metadata about the command execution.

- `application_name`: Name of the application (e.g., "SuperServer Automation Assistant")
- `version`: Application version (e.g., "1.4.0")
- `build_date`: Date the binary was built
- `architecture`: System architecture (e.g., "x86_64")
- `command`: Command string used for execution
- `schema_version`: Version of the output schema. This is a string in the format `saa-<SAA version>-<command name>-<command schema version>`
- `managed_system`: The system the tool is managing

data (optional): The actual response of the command, present only if no error. In some cases, both error and data prior to the error is also present.

- `data_type`: Type or category of data returned (e.g., "GetBmcInfo.ManagedSystem")
- Additional fields depend on the command used

messages (optional): Informational or warning messages.

- `timestamp`: Time the message was generated
- `severity`: Severity level (e.g., INFO, WARNING)
- `message`: Message text

error (optional): Present only on error.

- `exit_code`: Non-zero for error

- `description`: Summary of the error
- `program_error_code`: Tool-specific error identifier
- `error_message`: List of detailed errors
- `instruction`: User guidance for troubleshooting

Summary (optional): Present only for multi option.

- `executions`: Total number of execution attempts
- `success`: Number of successful executions
- `failed`: Number of failed executions
- `status_list`: Details for each execution, including start/end time, exit code, status, and system name

5. Managing Systems

5.1. License Management

5.1.1. Activating the Node Product Keys

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

1. Obtain a node product key from Supermicro. See 3.1 Getting Node Product Keys from Supermicro.
2. Use the following SAA command.

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

For Multiple Systems usage, the system list file format is fixed for the “ActivateProductKey” command, please refer to **4.4.2.1. ActivateProductKey Command**.

Example:

OOB:

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

[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":"11111111111111111112222222222
22222333333333333333abababababababababababbabcdcdcdcdcdcdcdccdcdcddcdefefe
fefefefefeefefefefghghghghghghghghghgh"}}'

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

In-Band:

```
[SAA_HOME]# ./saa -c ActivateProductKey --key 1111-1111-1111-1111-1111-
1111

[SAA_HOME]# ./saa -c ActivateProductKey --key '{"ProductKey":{"Node":
{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111112222222222
22222333333333333333abababababababababababbabcdcdcdcdcdcdcdccdcdcddcdefefe
fefefefefeefefefefghghghghghghghghghgh"}}'

[SAA_HOME]# ./saa -c ActivateProductKey --key_file mymacs.txt.key

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

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

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c ActivateProductKey --key 1111-1111-1111-1111-1111-1111 --remote_saa
/root/saa

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c ActivateProductKey --key_file mymacs.txt.key --remote_saa /root/saa
```

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c ActivateProductKey --key_file mymacs.txt.key --
remote_saa /root/saa
```

Multiple Systems OOB:

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

```
SList.txt:
    192.168.34.56 1111-1111-1111-1111-1111-1111
    192.168.34.57 ADMIN1 PASSWORD1 2222-2222-2222-2222-2222-2222
    192.168.34.58 {"ProductKey":{"Node":{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111111222222222222222333
33333333333abababababababababababbabcdcdcdcdcdcdccdcdcddcdefefefefefefefeefefef
efghghghghghghghghghgh"}}
```

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ActivateProductKey
--key_file mymacs.text.key
```

```
SList.txt:
    192.168.34.56
    192.168.34.57 ADMIN1 PASSWORD1
mymacs.text.key:
    003048001012;1111-1111-1111-1111-1111-1111-1111
    003048001015;{"ProductKey":{"Node":{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111111222222222222222333
33333333333abababababababababababbabcdcdcdcdcdcdccdcdcddcdefefefefefefefeefefef
efghghghghghghghghghgh"}}
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ActivateProductKey --
key_file mymacs.text.key --remote_saa /root/saa
```

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password
    192.168.34.58 OS_Username OS_PASSWD
mymacs.text.key:
    003048001012;1111-1111-1111-1111-1111-1111-1111
    003048001013;2222-2222-2222-2222-2222-2222-2222
    003048001015;{"ProductKey":{"Node":{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111111222222222222222333
```

```
33333333333abababababababababababbabcdcdcdcdcdcdcdccdcdcddcdefefefefefefefefeefefef
efghghghghghghghghghghgh"}}
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c ActivateProductKey --
key_file mymacs.text.key --remote_saa /root/saa
```

```
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
    192.168.34.58 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
mymacs.text.key:
    003048001012;1111-1111-1111-1111-1111-1111-1111
    003048001013;2222-2222-2222-2222-2222-2222-2222
    003048001015;{"ProductKey":{"Node":{"LicenseID":"1","LicenseName":"SFT-OOB-
LIC","CreateDate":"20200409"},"Signature":"11111111111111111111222222222222222333
33333333333abababababababababababbabcdcdcdcdcdcdcdccdcdcddcdefefefefefefefefeefefef
efghghghghghghghghghghgh"}}
```

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 1111-1111-1111-1111-1111-1111 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. For the third managed system 192.168.34.58, SAA applies -u ADMIN and -p PASSWORD to the command line and the HSM-supported node product key. These three 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
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 QueryProductKey
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c QueryProductKey
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -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

Remote In-Band:

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

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

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c QueryProductKey --
remote_saa /root/saa
```

```
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 QueryProductKey --
remote_saa /root/saa
```

```
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 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[1] (Dear Customer Letter) for each SKU in different product bundles.

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

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

5.1.3.1. CpuOnDemand Flow

1. Ensure your CPU[2] 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®.

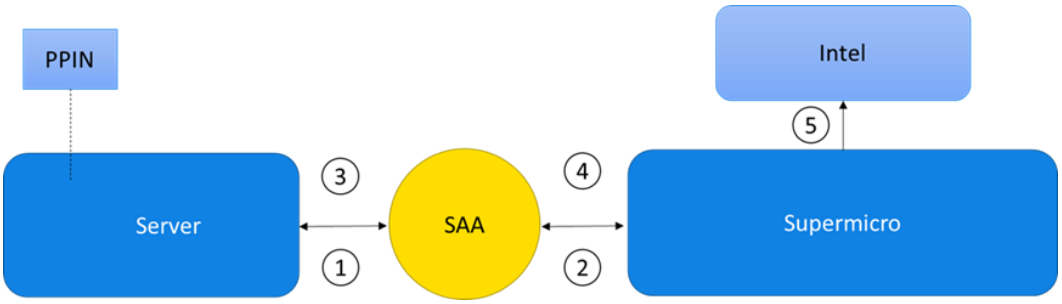


Figure 1 - CpuOnDemand Flow

[2] 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	**Communications & Storage Suite 4** QAT 4 Devices DLB 4 Devices DSA 4 Devices
XCC	99AV1V	AMS4	**Analytics Suite 4** IAX 4 Devices DSA 4 Devices
MCC	99AV1Z	CSS2	**Communications & Storage Suite 2** QAT 2 Devices DLB 2 Devices
MCC	99AV1R	AMS1	**Analytics Suite 1** IAX 1 Devices
ALL	99AV1P	SGX512	**SGX 512GB**

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]]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c CpuOnDemand --action GetHwInfo [--cpu_id <cpu_socket_id>] [--file < hw_id_file_name> [--overwrite]] [--remote_saa <remote saa path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CpuOnDemand --action GetHwInfo [--file < mlist_hw_id_file_name> [--overwrite]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c CpuOnDemand --action GetHwInfo [--file < mlist_hw_id_file_name> [--overwrite]] [--remote_saa <remote saa path>]

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    | AABBCCDD00112233  | 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 Redish_RHI -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
```

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c CpuOnDemand --action GetHwInfo --file hwidfile.txt -
-remote_saa /root/saa
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c CpuOnDemand --
action GetHwInfo --file hwidfile.txt
```

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c CpuOnDemand --action
GetHwInfo --file hwidfile.txt
```

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

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 -I Redfish_HI -u <username> -p <password> -c CpuOnDemand --action GetOnDemandState {--cpu_id <cpu_socket_id> | --hw_id <hw_id> | --hw_id_file <hw_id_file_name>} {[[-v]|[--squash]] [--file <StateReport> [--overwrite]] | --plain_text}
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS 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} [--remote_saa <remote saa path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CpuOnDemand --action GetOnDemandState [[[-v]|[--squash]] [--file

	<StateReport> [--overwrite]]] | [--plain_text]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c CpuOnDemand --action GetOnDemandState {[[-v]|[--squash]] [--file <StateReport> [--overwrite]] | --plain_text} [--remote_saa <remote saa path>]

For action GetOnDemandState, the system list file format is fixed, please refer to **4.4.2.7. CpuOnDemand Command**.

Example:

OOB:

```
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","stateCertificate":{"pendingCapabilityActivationPayloadCount":0,"value":"AaaaaBbbbbCcccc”}}],"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 treshold = 2
  - SDSi license key auth failure = 0
  - SDSi license key auth failure treshold = 2
  - SDSi updates available = 2
  - SDSi updates treshold = 2

Currently active:
  - SGX 512 EPC
```

```
Active after reboot:
```

In-Band:

a. [SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c CpuOnDemand --action GetOnDemandState --hw_id AABBCCDD00112233 --file DebugStateReport.json -v

The console output contains the following information.

```
Start reading the state report on CPU 0 of 169.254.3.254 system...
.................
Debug State Report has been successfully saved to the file <
DebugStateReport.json>.
```

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c CpuOnDemand --action GetOnDemandState --hw_id_file <hw_id_file_name> --file StateReport.json --remote_saa /root/saa

Multiple OOB:

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

```
SList.txt:
    192.168.34.56 AABBCCDD00112233
    192.168.34.57 ADMIN1 PASSWORD1 EEFFGGHH00112233
    192.168.34.57 ADMIN1 PASSWORD1 EEFFGGHH00445566
```

Multiple Systems Remote In-Band:

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c CpuOnDemand --action GetOnDemandState --plain_text

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_Password
AABBCCDD00112233
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_Password EEFFGGHH00112233
```

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]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c CpuOnDemand --action SetLicenseActivateCode --lac_file <LAC+.txt> [--reboot] [--remote_saa <remote saa path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CpuOnDemand --action SetLicenseActivateCode --lac_file <LAC+.txt> [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c CpuOnDemand ---action SetLicenseActivateCode --lac_file <LAC+.txt> [--reboot] [--remote_saa <remote saa path>]

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

The format of “LAC+.txt” is “<PPIN>;<LAC+ structure>” as an example below:

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

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p ADMIN -c CpuOnDemand --
action SetLicenseActivateCode --lac_file LAC+_AABBCCDD00112233.txt --
reboot
```

The console output contains the following information.

```
....
Start writing new LAC+ file on CPU 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+_AABBCCDD00112233.txt --reboot
```

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c CpuOnDemand --action SetLicenseActivateCode --
lac_file LAC+_ AABBCCDD00112233.txt --reboot --remote_saa /root/saa
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -c CpuOnDemand --action
SetLicenseActivateCode --lac_file LAC+_mlist.txt --reboot --post_complete
```

```
SList.txt:
    192.168.34.57 ADMIN PASSWORD
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c CpuOnDemand --action
SetLicenseActivateCode --lac_file LAC+_mlist.txt --reboot
```

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

4. Syntax of EnablePPIN:

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

	CpuOnDemand --action EnablePPIN --reboot [--post_complete]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c CpuOnDemand --action EnablePPIN --reboot
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c CpuOnDemand --action EnablePPIN --reboot [--remote_saa <remote saa path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CpuOnDemand --action EnablePPIN --reboot [--post_complete]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c CpuOnDemand --action EnablePPIN --reboot [--remote_saa <remote saa path>]

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

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c CpuOnDemand --action EnablePPIN --reboot --
remote_saa /root/saa
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -c CpuOnDemand --action EnablePPIN --
reboot --post_complete
```

```
SList.txt:
    192.168.34.57 ADMIN PASSWORD
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c CpuOnDemand --action
EnablePPIN --reboot
```

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

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-OOB-LIC
    SFT-DCMS-SINGLE
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. With the --file option, the asset information can be saved in the log.txt file.

Single System

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

Example:

OOB:

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

Multiple OOB:

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

```
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: OA182S021066
                    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.

Option Commands	Descriptions
--action	Sets action to: 1 = Show 2 = Del 3 = GetVer 4 = SetVer



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.”
- The Redfish protocol supports only the [--action Show] option.

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>]] [--redfish] [--temp_unit <unit>] [--showall]

In-Band	saa -c CheckSensorData [-I Redfish_HI -u <username> -p <password>] [--action <action> [--sdr_id <id>] [--sdr_major_version <version> --sdr_minor_version <version>]] [--showall]
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 CheckSensorData [--action <action> [--sdr_id <id>] [--sdr_major_version <version> --sdr_minor_version <version>]] [--showall]
Multiple Systems	
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>]] [--redfish] [--temp_unit <unit>] [--showall]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c CheckSensorData [--action <action> [--sdr_id <id>] [--sdr_major_version <version> --sdr_minor_version <version>]] [--redfish] [--temp_unit <unit>] [--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
```

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

For the CPU temperature sensor, **the console output displays the temperature in Fahrenheit as the unit 'F' was provided**

```
Status | (#)Sensor                |      Reading |    Low NR |    Low CT |    Low
NC |   High NC |   High CT |   High NR |
------ | ---------                |      ------- |    ------ |    ------ |    ---
--- |   ------- |   ------- |   ------- |
OK     | (4) CPU Temp             |         108F |       41F |       41F |
50F |      210F |      219F |      219F |
```

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

For the BMC sensor, **the console output contains the following information.**

```
Status    | (#)Sensor   |   Reading |   Lower Caution | Lower Critical |    Lower
Fatal |   Upper Caution | Upper Critical |    Upper Fatal |
------    | ---------   |   ------- | --------------- | -------------- |    -----
------ | --------------- | -------------- |    ------------ |
OK        | (#)BMC 1.0V |    1.014V |          0.000V |         0.887V |
0.000V |          0.000V |         1.092V |         0.000V |
```

In-Band:

```
[SAA_HOME]# ./saa -c CheckSensorData --action Show
```

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

```
Status | (#)Sensor                |      Reading | Low Limit | High Limit |
------ | ---------                |      ------- | --------- | ---------- |
OK     | (4) CPU Temp             |     42C/108F |    5C/41F |  104C/219F |
```

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

For the VBAT sensor, **the console output contains the following information.**

```
Status | (#)Sensor                |      Reading | Low Limit | High Limit |
------ | ---------                |      ------- | --------- | ---------- |
OK     | (#)VBAT                  |         Battery Presence Detected     |
```

Remote In-Band:

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

```
[SAA_HOME]#./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c CheckSensorData --action Show --showall --remote_saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]#./saa -I Remote_INB -l SList.txt -c CheckSensorData --action
GetVer --remote_saa
```

```
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 CheckSensorData --action
Show --showall --remote_saa
```

```
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 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
Multiple Systems	
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>}
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 ServiceCalls {--file <servicecalls XML file>}
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c ServiceCalls {--file <servicecalls XML file>}
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -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
```

Remote In-Band:

```
./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c
ServiceCalls --file current.xml --remote_saa /root/saa
```

```
./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p
ADMIN -c ServiceCalls --file current.xml --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ServiceCalls --file
<servicecalls XML file> --remote_saa /root/saa
```

```
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 ServiceCalls --file
<servicecalls XML file> --remote_saa /root/saa
```

```
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 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 receipient’s e-mail address (“RecipientEmail”) is genunine and correct, the status of HW events will be sent to the recipient’s e-mail address. The default “RecipientEmail” e-mail is “*hwevent_alert@supermicro.com*”.

- Recipient Information node - <Recipient_Information> (Required)
  This section allows user to fill out the recipient's information, such as his/her name ("Name") and his/her title ("Role") in each node and set the recipient's e-mail addresss in the node to receive alerts classified as non-HW events.

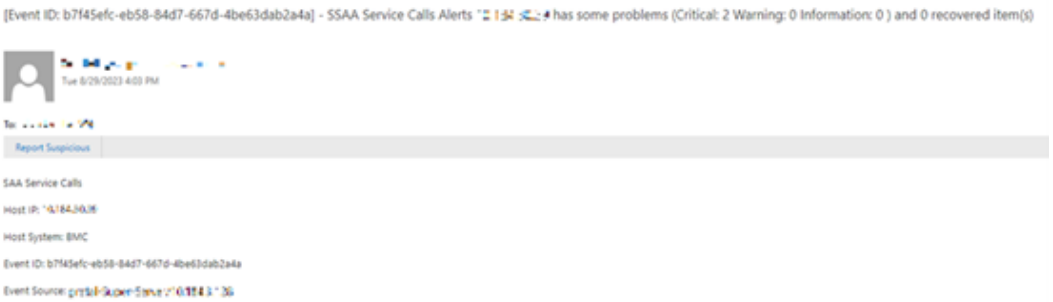
- Customer Information node - <Customer_Information>
  You can fill out the information of the customer applying for ServiceCalls service, such as name and company.

- Site Location Information node - <Site_Location_Information>
  You can mention where the managed system is located. Besides company name and address, the contact information can be filled out for further action.

Notes:

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

5.2.5.2. Email Format



The e-mail content includes:

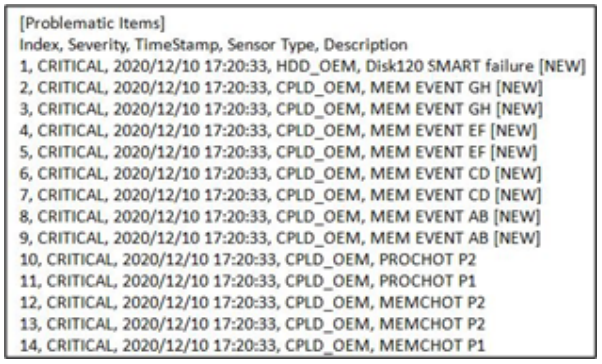
- **Subject Line**
  Contains Event ID, function name, the managed system BMC/CMM IP, and the summary of the host.

- **Body**

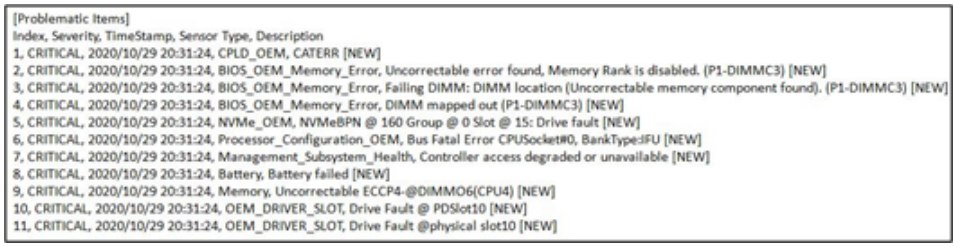
  - **E-mail Function:** It is “SAA Service Calls” in this example.
  - **Host IP:** The BMC/CMM IP address of the managed system.
  - **Event ID:** The 32 bytes of GUID.
  - **Event Source:** The OS IP address of the managing system.

- **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 definedby 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.”

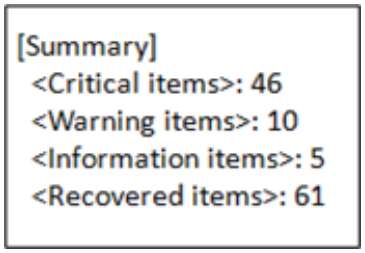

[Problematic Items]
Index, Severity, TimeStamp, Sensor Type, Description
1, CRITICAL, 2020/10/29 20:31:24, CPLD_OEM, CATERR [NEW]
2, CRITICAL, 2020/10/29 20:31:24, BIOS_OEM_Memory_Error, Uncorrectable error found, Memory Rank is disabled. (P1-DIMMC3) [NEW]
3, CRITICAL, 2020/10/29 20:31:24, BIOS_OEM_Memory_Error, 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 CPUSocket#0, BankType:IFU [NEW]
7, CRITICAL, 2020/10/29 20:31:24, Management_Subsystem_Health, Controller access degraded or unavailable [NEW]
8, CRITICAL, 2020/10/29 20:31:24, Battery, Battery failed [NEW]
9, CRITICAL, 2020/10/29 20:31:24, Memory, Uncorrectable ECCP4-@DIMMO6(CPU4) [NEW]
10, CRITICAL, 2020/10/29 20:31:24, OEM_DRIVER_SLOT, Drive Fault @ PDSlot10 [NEW]
11, CRITICAL, 2020/10/29 20:31:24, OEM_DRIVER_SLOT, Drive Fault @physical slot10 [NEW]

- **Recovered Items (Last Check):**
  This section contains the SEL and SDR items previously marked as problematic items but later recovered in the last check.



- **Summary:**

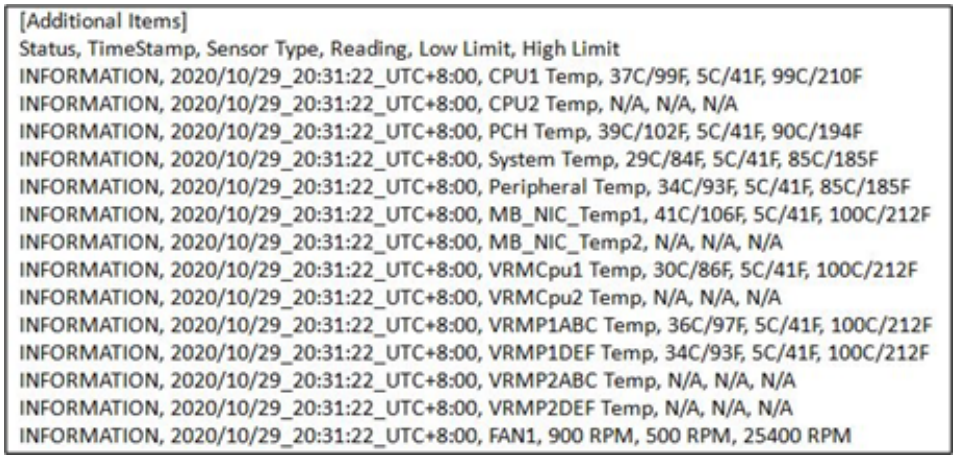
  The number of both problematic and recovered items are shown in the Summary.



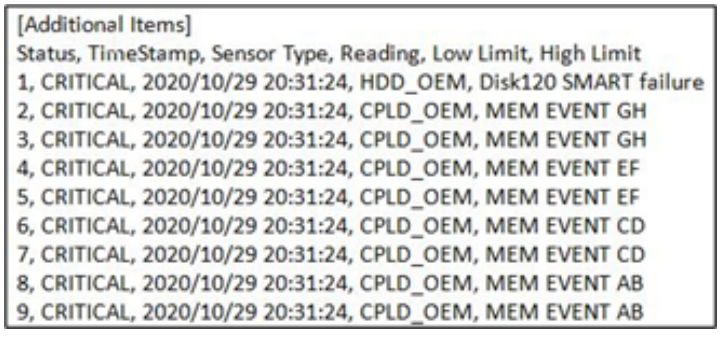
- **Additional Items:**

  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.



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



- **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, Adminstrator
          Email: 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
```

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]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c SystemPFA {--action <action>} [--reboot]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SystemPFA {--action <action>} [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c SystemPFA {--action <action>} [--reboot]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c SystemPFA --action Disabled --reboot --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SystemPFA --action
Disabled --reboot --remote_saa /root/saa
```

```
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 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 -I Redfish_HI -u <username> -p <password> -c MemoryHealthCheck {--action <action>} [--reboot]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS 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]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c MemoryHealthCheck {--action <action>} [--reboot]

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 -I Redfish_HI -u ADMIN -p PASSWORD -c MemoryHealthCheck --action Enable --reboot

In-Band:

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c MemoryHealthCheck --action Enable --reboot --remote_saa /root/saa

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c MemoryHealthCheck --
action Enable --reboot --remote_saa /root/saa
```

```
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 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}
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 chassisIntrusion --action {Clear | Status} [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l < system list file > [-u <username> -p <password>] -c ChassisIntrusion --action {Clear | Status}
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c ChassisIntrusion --action {Clear | Status} [--remote_saa <remote SAA path>]

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..............192.168.34.56
Intrusion Sensor.........Normal
```

In-band:

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

Remote In-Band:

```
[SAA_HOME]# sudo ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op
111111 -c ChassisIntrusion --action Clear --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ChassisIntrusion --action
status
```

```
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 ChassisIntrusion --action
status
```

```
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 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 [--post_complete]
Multiple Systems	

OOB	saa -l <system list file> -c SuperDiag --action Start --file --image_url <URL of ISO image> [--dev_id <index>] --reboot [--post_complete]

• 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 --post_complete

[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.



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.

5.2.10.1. 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 [--post_complete]
In-Band	saa -I Redfish_HI -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 -I Redfish_HI -u <username> -p <password> -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 dianostics results.

Example:

OOB:

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

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

In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SuperDiag --
action Start --embedded --reboot
```

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SuperDiag --
action Download --embedded --file results.html
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SuperDiag --action
Start --embedded --reboot --post_complete
```

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

```
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.

5.2.11. 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SendDiagInterrupt
In-Band	saa -c SendDiagInterrupt
Multiple Systems	
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. 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>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c TasManage --action <action> [--period <update period>] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c TasManage --action <action> [--period <update period>]
Remote In-Band	saa -I Remote_INB -l <system list file> -c TasManage --action <action> [--period <update period>] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

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

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c TasManage --action Pause
```

```
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 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.

5.2.13. 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CheckSelfTest
In-Band	saa -c CheckSelfTest
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c CheckSelfTest
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CheckSelfTest
Remote In-Band	saa -I Remote_INB -l <system list file> -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
```

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

```
........
Self Test function not implemented in this controller
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
[Controller operational firmware corrupted]
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Corrupted or inaccessible data or device
[Controller update boot block corrupted]
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Corrupted or inaccessible data or device
[Internal Use Area corrupted]
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Corrupted or inaccessible data or device
[SDR repository empty]
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Corrupted or inaccessible data or device
[IPMB signal lines do not respond]
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Corrupted or inaccessible data or device
[FRU device not accessible]
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Corrupted or inaccessible data or device
[SDR repository not accessible]
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Corrupted or inaccessible data or device
[SEL device not accessible]
```

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Fatal hardware error
```

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

```
SuperServer Automation Assistant 1.0.0 (2024/02/05) (x86_64)
Copyright(C) 2023-2024 Super Micro Computer, Inc. All rights reserved.
........
Device specific, CCh
```

Remote In-Band:

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

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c CheckSelfTest --
remote_saa /root/saa
```

```
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 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. 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 = GetCurrentStatus 2 = Enable 3 = Disable

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c HDTService --action <action>
In-Band	saa -I Redfish_HI -u <username> -p <password> -c HDTService --action <action>
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c HDTService --action <action> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c HDTService --action <action>

Remote In-Band	saa -I Remote_RHI -l <system list file> -c HDTService --action <action> [--remote_saa <remote SAA path>]

Example:

OOB:

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

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.
```

Remote In-Band:

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

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c HDTService --action
GetCurrentStatus --remote_saa /root/saa
```

```
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 "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.
- The FRU version will be displayed if the managed system supports it.

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] [--json_view] saa -i <IP or host name> -u <username> -p <password> -c GetFruInfo

	[--file <filename> --dump [--format <file format>] [--overwrite]] [--redfish] [--json_view]
In-Band	saa -c GetFruInfo [-I Redfish_HI -u <username> -p <password>] [--file <filename> {--dump [--format <file format>] [--overwrite] | --file_only}] [--dev_id <Device ID>] | [--showall] [--json_view] saa -c GetFruInfo [-I Redfish_HI -u <username> -p <password>] [--file <filename> {--dump [--format <file format>] [--overwrite] | --file_only}] [--redfish] [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetFruInfo [--file <filename> --dump [--format <file format>] [--overwrite]] [--json_view] [--remote_saa <remote SAA path>] saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetFruInfo [--file <filename> --dump [--format <file format>] [--overwrite]] [--redfish] [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetFruInfo [--file <filename> --dump [--format <file format>] [--overwrite]] [--dev_id <Device ID>] | [--showall] [--json_view] saa -l <system list file> [-u <username> -p <password>] -c GetFruInfo [--file <filename> --dump [--format <file format>] [--overwrite]] [--redfish] [--json_view]
Remote In-Band	saa -I Remote_INB <system list file> -c GetFruInfo [--file <filename> --dump [--format <file format>] [--overwrite]] [--json_view] [--remote_saa <remote SAA path>] saa -I Remote_RHI <system list file> -c GetFruInfo [--file <filename> --dump [--format <file format>] [--overwrite]] [--redfish] [--json_view] [--remote_saa <remote SAA path>]

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]
        Chassis Type (CT): 01
        Chassis Part Number (CP):
        Chassis Serial Number (CS):
        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):
```

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

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

The console output contains the following information.

```
FRU information [Version=00.00]
================================
    [BMC, ID=0, Size=256 bytes]
        Chassis Type (CT): 00
        Chassis Part Number (CP):
        Chassis Serial Number (CS):
```

```
        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):
```

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

The console output contains the following information.

```
FRU information
================================
    [BMC, ID=0]
        Board mfg. Date/Time (BDT): 1996/01/01 00:00
        Board Manufacturer Name (BM): Supermicro
        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):
```

Remote In-band:

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

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

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.

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetFruInfo --remote_saa
/root/saa
```

```
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 GetFruInfo --remote_saa
/root/saa
```

```
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
```

5.3.1.2 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>}
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c ChangeFruInfo {--item <item name> --value <assignment value> | --fru_version <FRU version>} [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeFruInfo {--item <item name> --value <assignment value> | --fru_version <FRU version>}
Remote In-Band	saa -I Remote_INB -l <system list file> -c ChangeFruInfo {--item <item name> --value <assignment value> | --fru_version <FRU version>} [--remote_saa <remote saa path>]

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):
```

Remote In-band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c ChangeFruInfo --item CT --value 0x01 --remote_saa /root/saa
```

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
    192.168.34.57
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ChangeFruInfo --item CT -
-value 0x01 --remote_saa /root/saa
```

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

5.3.2. Getting System Summary Firmware Image Information

Use the "GetSystemInfo" command to retrieve comprehensive firmware image information from the managed system.

Without the "--redfish" option, this command provides a system-wide summary, encompassing firmware details of components, including System, LAN, BMC, BIOS, CPLD, SCP and Redfish version, if supported.

With the "--redfish" option, the "GetSystemInfo" command retrieves systems and chassis information through the Redfish protocol.



Notes:

- For NVIDIA systems, the "GetSystemInfo" command only supports the Redfish protocol. For in-band access, please use the Redfish host interface with the "-I Redfish_HI" option.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetSystemInfo [--redfish] [--json_view]
In-Band	saa -c GetSystemInfo [--json_view] saa -I Redfish_HI [-u <username> -p <password>] -c GetSystemInfo [--redfish] [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetSystemInfo [--json_view] [--remote_saa <remote SAA path>] saa -I Remote_RHI [-u <username> -p <password>] --oi <OS IP address> --ou <OS username> --op <OS password> -c GetSystemInfo [--redfish] [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetSystemInfo [--redfish] [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetSystemInfo [--json_view] [--remote_saa <remote SAA path>] saa -I Remote_RHI -l <system list file> -c GetSystemInfo [--redfish] [--json_view] [--remote_saa <remote SAA path>]

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:EFFF: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:EFFF: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:EFFF: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
```

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

The console output contains the following information.

```
System information
==============================
[System]
    [System_0]
        Location:
            LocationType:
            ServiceLabel:
        Identify LED: Lit
        Serial number:
        Part number:
        Model:
        Asset tag:
        Manufacturer:
        Description: Computer System
        Sub model:
        System type: Physical
        Status (State): Disabled
        Power: PoweringOff
        Health: OK
        Health rollup:
        Memory summary
            Total system memory: 0 GiB
            Processor summary
            Count: 0
                Core count: 0


Chassis information
==============================
[BMC]
    [BMC_0]
        Location:
            LocationType: Embedded
```

```
            ServiceLabel:
        Identify LED: Lit
        Part number: AOM-SCM-NV2
        Serial number: $BOARD_SERIAL_NUMBER
        Model: BMC Secure Control Module
        Asset tag:
        Manufacturer: Supermicro
        Chassis type: Component
        Status (State): StandbyOffline
        Power: Off
        Health: OK
        Health rollup: OK
        Min power: 0 W
        Max power: 0 W
```

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

The console output contains the following information.

```
File "SystemInfo.json" is created.
```

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 GetSystemInfo
```

Multiple Systems OOB:

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

```
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 GetSystemInfo
```

```
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.

5.3.3. 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 acessed.
- A configuration file in XML can be downloaded from CMM through the --download option. The feature is only supported by 64MB CMM AST2400.
- For details on profile update, please refer to 5.7.16 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]]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetSystemCfg --file <SystemCfg.xml> [--overwrite] [[--download] [--file_id]] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetSystemCfg --file <SystemCfg.xml> [--overwrite] [[--download] [--file_id]]

Remote In-Band	saa -I Remote_INB -l <system list file> -c GetSystemCfg --file <SystemCfg.xml> [--overwrite] [[--download] [--file_id]] [--remote_saa <remote SAA path>]

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
```

In-Band:

```
[SAA_HOME]# ./saa -c GetSystemCfg --file SystemCfg.xml --overwrite
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c GetSystemCfg --file SystemCfg.xml --overwrite --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetSystemCfg --file SystemCfg.xml --overwrite --remote_saa /root/saa
```

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

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]]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c ChangeSystemCfg [[--update Apply|Deploy --dev_id <Device ID> --file_id <file ID> --reboot] | [--upload --file SystemCfg.xml]] [--remote_saa <remote SAA path>]
In-band	saa -c ChangeSystemCfg --file <SystemCfg.xml> [--reboot]
Multiple Systems	
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]]
Remote In-Band	saa -I Remote_INB -l <system list file> -c ChangeSystemCfg [[--update Apply|Deploy --dev_id <Device ID> --file_id <file ID> --reboot] | [--

	upload --file SystemCfg.xml]] [--remote_saa <remote SAA path>]

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
```

In-Band:

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

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c ChangeSystemCfg --file SystemCfg.xml --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ChangeSystemCfg --file
SystemCfg.xml --remote_saa /root/saa
```

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

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
8	PUE Optimal
9	Smart Cooling
10	Performance
11	Silent

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> --fanspeed <fan speed value> --zone <zone value> --pwm <pwm value>
In-band	saa -c SetFanMode --fanmode <fan type> --fanspeed <fan speed value> --zone <zone value> --pwm <pwm value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SetFanMode > --fanspeed <fan speed value> --zone <zone value> --pwm <pwm value>

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
```

```
[SAA_HOME]# ./saa -c setfanmode --fanmode 1 --fanspeed 50 -i 172.31.32.54 -u root -p 0penBmc --zone 1 --pwm 1
```

The console output contains the following information.

```
Fan mode is changed to manual.
Fan speed is changed to 50 % for Zone1 and PWM1
All Available Fan Modes are:
Mode: Type
0: Auto
1: Manual
```

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
```



Note: Fan speed, zone, PWM are only available on NVIDIA systems.

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: 1 = GetStatus 2 = On 3 = Off

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

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 [--post_complete]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c ClearCMOS --ac_cycle
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c ClearCMOS --ac_cycle [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l < system list file > [-u <username> -p <password>] -c ClearCMOS --ac_cycle [--post_complete]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c ClearCMOS --ac_cycle [--remote_saa <remote SAA path>]

Example:

OOB:

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

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
```

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 ClearCMOS --ac_cycle
```

Multiple systems OOB:

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

```
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
```



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	saa -i <IP or host name> -u <username> -p <password> -c GetBiosInfo [--showall] [--extract_measurement]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetBiosInfo [--file <filename> [--file_only]] [--showall] [--extract_measurement]
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 GetBiosInfo [--file <filename> [--file_only]] [--showall] [--extract_measurement] [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBiosInfo [--file <filename>] [--showall]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c GetBiosInfo [--file <filename>] [--showall] [--remote_saa <remote SAA path>]

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
6D97F0F3D9DB5945E0D0DFD59F8511F6857E915B414A1B9A30071EF5D99018144033DCC80464B951E
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 [-I Redfish_HI -u <username> -p <password>] -c UpdateBios --file <filename> [options…]
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 UpdateBios --file <filename> [--remote_saa <remote SAA path>] [options…]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateBios --file <filename> [options…]
Remote In-Band	saa {-I Remote_INB | -I 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.
- The OOB BIOS update feature is not supported on some X13, X12 and B4 motherboards that implement client ME such as X13SAE, X13SAZ, B4SA1, X12SAE, X12SCA and X12SCZ.
- 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 4.3.3 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 o 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.
- If receiving the exit code 254 in In-Band mode, you should reboot the system and execute the same command again.
    - Users can also write a script to automate the procedure in Remote In-Band Mode.
        a. Execute UpdateBIOS command in Remote In-Band mode.
        b. Execute the system reboot command when SAA returns Exit Code 254.
        c. Ping the OS IP until the OS responses.
        d. Execute the UpdateBIOS command in Remote In-Band mode again.

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.
- Use "--filter nondefault" option to generate a BIOS configuration file that includes only the settings where the current values differ from the defaults.
- Use "--tui" option to view BIOS configuration in a text-based user interface (TUI). For details, refer to 4.9 TUI.
- Use "--compact" option to generate a compact version of the BIOS configuration file in TUI by removing 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	saa -i <IP or host name> -u <username> -p <password> -c GetCurrentBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--current_password <current password> | --cur_pw_file <current password file path>] [--filter <filter type>] [--tui [--compact]]
In-Band	saa -c GetCurrentBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--current_password <current password> | --cur_pw_file <current password file path>] [--filter <filter type>] [--tui [--compact]]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetCurrentBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--current_password <current password> | --cur_pw_file <current password file path>] [--filter <filter type>] [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c GetCurrentBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--filter <filter type>]
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetCurrentBiosCfg [--file <USER_SETUP.file> [--overwrite]] [--filter <filter type>] [--remote_saa <remote SAA path>]

For Multiple Systems usage, the system list file format is fixed for the "GetCurrentBiosCfg" command, please refer to **4.4.2.3. BIOS Configuration Related Commands**.

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 --filter nondefault

Remote In-Band:

[SAA_HOME]# ./saa -I 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 --overwrite

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

Multiple Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetCurrentBiosCfg --file USER_SETUP.file --overwrite

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD current_password
    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 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	saa -i <IP or host name> -u <username> -p <password> -c ChangeBiosCfg --file <current.file> [--current_password <current password> | --cur_pw_file <current password file path>] [--reboot [--post_complete]]
In-Band	saa -c ChangeBiosCfg --file <current.file> [--current_password <current password> | --cur_pw_file <current password file path>] [--

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

For Multiple Systems usage, the system list file format is fixed for the “ChangeBiosCfg” command, please refer to **4.4.2.3. BIOS Configuration Related Commands**.

Example:

OOB:

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

In-Band:

[SAA_HOME]# ./saa -c ChangeBiosCfg --file current.file --reboot

Remote In-Band:

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

Multiple Systems OOB:

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeBiosCfg --file current.file --reboot
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c ChangeBiosCfg --file current.file --reboot --individually

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

Multiple Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ChangeBiosCfg --file current.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: current.file.192.168.34.56 and current.file.192.168.34.57. Then set the --file argument with the “current.file” file name. With the --individually option, SAA searches for current.file.192.168.34.56 and current.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 default.file file.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetDefaultBiosCfg [--file <default.file> [--overwrite]] [--current_password <current password> | --cur_pw_file <current password file path>]
In-Band	saa -c GetDefaultBiosCfg [--file <default.file> [--overwrite]] [--current_password <current password> | --cur_pw_file <current password file path>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetDefaultBiosCfg [--file <default.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 <default.file> [--overwrite]]
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetDefaultBiosCfg [--file <default.file> [--overwrite]] [--remote_saa <remote SAA path>]

For Multiple Systems usage, the system list file format is fixed for the "GetDefaultBiosCfg" command, please refer to **4.4.2.3. BIOS Configuration Related Commands**.

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 default.file --overwrite

Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111-c GetDefaultBiosCfg --file default.file --overwrite --remote_saa /root/saa

Multiple Systems OOB:

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetDefaultBiosCfg --file default.file

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

Multiple Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetDefaultBiosCfg --file default.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., default.file.192.168.34.56. The --overwrite option is used to force overwrite the existing file, e.g., default.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	saa -i <IP or host name> -u <username> -p <password> -c LoadDefaultBiosCfg [--current_password <current password> | --cur_pw_file <current password file path>] [--reboot [--post_complete]] [--redfish]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c LoadDefaultBiosCfg [--current_password <current password> | --cur_pw_file <current password file path>] [--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 LoadDefaultBiosCfg [--optimized_default] [--current_password <current

	password> | --cur_pw_file <current password file path>] [--reboot] [--remote_saa <remote SAA path>] [--redfish]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c LoadDefaultBiosCfg [--reboot [--post_complete]] [--redfish]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c LoadDefaultBiosCfg [--reboot] [--remote_saa <remote SAA path>] [--redfish]

For Multiple Systems usage, the system list file format is fixed for the "LoadDefaultBiosCfg" command, please refer to **4.4.2.3. BIOS Configuration Related Commands**.

Example:

OOB:

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c LoadDefaultBiosCfg --reboot

In-Band:

```
[SAA_HOME]# ./saa -c LoadDefaultBiosCfg --reboot
```

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

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c LoadDefaultBiosCfg --reboot

Multiple Systems OOB:

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

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

Multiple Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c LoadDefaultBiosCfg --reboot

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

Multiple Remote In-Band Redfish Host Interface:

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt.txt -c LoadDefaultBiosCfg --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
```

5.4.8. 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	saa -i <IP or host name> -u <username> -p <password> -c GetDmiInfo [--file <DMI.txt> [--overwrite]]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetDmiInfo [--file <DMI.txt> [--overwrite]]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetDmiInfo [--file <DMI.txt> [--overwrite]][--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetDmiInfo [--file <DMI.txt> [--overwrite]]
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetDmiInfo [--file <DMI.txt> [--overwrite]] [--remote_saa <remote SAA path>]

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	saa -i <IP or host name> -u <username> -p <password> -c EditDmiInfo {--file <DMI.txt> --item_type <Item Type> --item_name <Item Name> | --shn <Item Short Name>} {--value <Item Value> | --default}
In-Band	saa -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 --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>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c EditDmiInfo {--file <DMI.txt> --item_type <Item Type> --item_name <Item Name> | --shn <Item Short Name>} {--value <Item Value> | --default}
Remote In-Band	saa -I Remote_INB -l <system list file> -c EditDmiInfo {--file <DMI.txt> --item_type <Item Type> --item_name <Item Name> | --shn <Item Short Name>} {--value <Item Value> | --default} [--remote_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 -l <system list file> [-u <username> -p <password>] -c ChangeDmiInfo {--file <DMI.txt>} [--reboot [--post_complete]] [--individually]
Remote In-Band	saa -I Remote_INB -l <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>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SetBiosPassword [{--new_password <new password> --confirm_password <confirm password> | --pw_file <password file path>} [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_INB -l <system list file> -c SetBiosPassword [{--new_password <new password> --confirm_password <confirm password> | --pw_file <password file path>} [--reboot] [--remote_saa <remote SAA path>]

For Multiple Systems usage, the system list file format is fixed for the "SetBiosPassword" command, please refer to **4.4.2.2. SetBiosPassword Command**.

Example:

OOB:

[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
```

Multiple Systems OOB:

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

```
SList.txt:
    192.168.34.56 new_password current_password
    192.168.34.57 new_password current_password
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetBiosPassword --reboot
```

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

If the execution “Status” field of the managed system shows SUCCESS, the console output of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

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 Redfish_HI -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 -I 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 [-I Redfish_HI -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 -l <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 [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetScpInfo [--json_view]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetScpInfo [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetScpInfo [--json_view]
Remote In-Band	saa -I Remote_RHI -l < system list file > -c GetScpInfo [--json_view]

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
```

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 GetScpInfo
```

Multiple Systems OOB:

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

```
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 GetScpInfo
```

```
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
```



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 -I Redfish_HI -u <username> -p <password> -c UpdateScp --file <filename> --reboot
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateScp --file <filename> --reboot [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateScp --file <filename> --reboot [--post_complete]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c UpdateScp --file <filename> [--remote_saa <remote SAA path>]

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.
```

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 UpdateScp --file scp_image.tar --reboot
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateScp --file
scp_image.tar --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.

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c UpdateScp --file
scp_image.tar --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
```

5.4.16. 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]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetFixedBootCfg [--file <filename>] [--overwrite]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetFixedBootCfg [--file <filename>] [--overwrite]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetFixedBootCfg --file <USER_SETUP.file> [--overwrite]
>Remote In-Band	saa -I Remote_RHI -l <system list file> [-u <username> -p <password>] -c GetFixedBootCfg --file <USER_SETUP.file> [--overwrite]

Example:

OOB:

```
./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetFixedBootCfg --file
FixedBootCfg.xml --overwrite
```

In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c GetFixedBootCfg --
file FixedBootCfg.xml --overwrite
```

Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c GetFixedBootCfg --file FixedBootCfg.xml --overwrite
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l Slist.txt -u ADMIN -p PASSWORD -c GetFixedBootCfg --
file USER_SETUP.file --overwrite
```

```
Slist.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Remote In-Band Redfih Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l IP_ADDR_RANGE.txt -c GetFixedBootCfg -
-file FixedBootCfg.xml --overwrite
```

```
IP_ADDR_RANGE.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
```

5.4.17. 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 UEFINetwork devices in the “UefiNetworkBBSPriorities” menu change their orders after the "Fixed Boot Order" menu in <setting selectedOption=UEFI Network> option shows the device of the first priority that you change in the “UefiNetworkBBSPriorities” menu. But you cannot change the UEFI Network display device in the "Fixed Boot Order" menu directly.

- 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]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c ChangeFixedBootCfg --file <USER_SETUP.file> [--reboot]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeFixedBootCfg --file <USER_SETUP.file> [--reboot [--post_complete]] [--individually]

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
```

Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c ChangeFixedBootCfg --file FixedBootCfg.xml
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l Slist.txt -u ADMIN -p PASSWORD -c ChangeFixedBootCfg
--file USER_SETUP.file --reboot

[SAA_HOME]# ./saa -l Slist.txt -u ADMIN -p PASSWORD -c ChangeFixedBootCfg
--file USER_SETUP.file --reboot --individually
```

```
Slist.txt:
    192.168.34.56
    192.168.34.57
```

Multiple Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l IP_ADDR_RANGE.txt -c
ChangeFixedBootCfg --file FixedBootCfg.xml
```

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 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
    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, and Device Type settings. If you do not use the "--next_boot_only" options, the default value will be "Enable." 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>] [--action <action> [--post_complete]]
In-Band	saa -c SetBootOption --device_type <Device Type ID> [--next_boot_only <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>] [--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 –-action 5
```

In-Band:

```
[SAA_HOME]# ./saa -c SetBootOption -c SetBootOption --device_type 0 --
next_boot_only 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 –-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 <current password file path>] [--boot_lan <boot lan port>] [--boot_name <boot description>] --image_url <URL> [--reboot [--post_complete]] [--file <file name>] saa -i <IP or host name> -u <username> -p <password> -c SetHttpBoot [--current_password <current password> | --cur_pw_file <current password file path>] --boot_clean [--reboot [--post_complete]]
In-Band	saa -c SetHttpBoot [--current_password <current password> | --cur_pw_file <current password file path>] [--boot_lan <boot lan port>] [--boot_name <boot description>] --image_url <URL> [--reboot] [--file <file name>] saa -c SetHttpBoot [--current_password <current password> | --cur_pw_file <current password file path>] --boot_clean [--reboot]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SetHttpBoot [--current_password <current password> | --cur_pw_file <current password file path>] [--boot_lan <boot lan port>] [--boot_name <boot description>] --image_url <URL> [--reboot] [--file <file name>] [--remote_saa <remote SAA path>] saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SetHttpBoot [--current_password <current password> | --cur_pw_file <current password file path>] --boot_clean [--reboot] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SetHttpBoot [--boot_lan <boot lan port>] [--boot_name <boot description>] --image_url <URL> [--reboot [--post_complete]] [--file <file name>]

	saa -l <system list file> [-u <username> -p <password>] -c SetHttpBoot --boot_clean [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_INB -l <system list file> -c SetHttpBoot [--boot_lan <boot lan port>] [--boot_name <boot description>] --image_url <URL> [--reboot] [--file <file name>] [--remote_saa <remote SAA path>] saa -I Remote_INB -l <system list file> -c SetHttpBoot --boot_clean [--reboot] [--remote_saa <remote SAA path>]

For Multiple Systems usage, the system list file format is fixed for the “SetHttpBoot” command, please refer to **4.4.2.3. BIOS Configuration Related Commands**.

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c SetHttpBoot --boot_name bootDescription --image_url
http://192.168.12.78/iso/efishell.iso --reboot --remote_saa /root/saa

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

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

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.

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetHttpBoot --boot_name
bootDescription --image_url http://192.168.12.78/iso/efishell.iso --
reboot --remote_saa /root/saa
```

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -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 -
-remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetHttpBoot --boot_clean
--reboot --remote_saa /root/saa
```

```
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:

- 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 [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetBiosPostCode [--json_view]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetBiosPostCode [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBiosPostCode [--json_view]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetBiosPostCode [--json_view][--remote_saa <remote SAA path>]

Example:

OOB:

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

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

In-Band through Redfish Host Interface:

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

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

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 --
remote_saa /root/saa
```

```
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 [-I Redfish_HI -u <username> -p <password>] -c GetBmcInfo [--file <filename> [--extract_measurement]] [--showall]
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 GetBmcInfo [--file <filename> [--extract_measurement]] [--showall]

Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetBmcInfo [--file <filename> [--extract_measurement]] [--showall]
Remote In-Band	saa -I 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 OOB:

```
[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 4.3.3 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] [--no_waiting]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl] [--no_waiting]
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>] [--no_waiting]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl] [--no_waiting]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr] [--backup] [--forward] [--overwrite_ssl] [--remote_saa <remote SAA path>] [--no_waiting]

Example:

OOB:

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

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateBmc --no_waiting --file BMC_X12AST2600-ROT-5201MS_20240715_01.04.09_STDsp.bin
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.4.0 (2025/06/04) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.

Managed system..........192.168.34.56
    BMC type............X12_RoT_ATEN_AST2600
    BMC version.........01.04.09
    BMC ext. version.....01 00 00 (P)
    BMC build date.......2024/07/15
Local BMC image file.....BMC_X12AST2600-ROT-5201MS_20240715_01.04.09_STDsp.bin
    BMC UFFN............BMC_X12AST2600-ROT-5201MS_20240715_01.04.09_STDsp.bin
    BMC type............X12_RoT_ATEN_AST2600
    BMC version.........01.04.09
    BMC build date.......2024/07/15
    FW image............Signed
        Signed Key.......RoT

Status: Start updating BMC for 192.168.34.56

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

```
Uploading FW.........................Done
Updating FW...>>>
```

```
[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
Inband	./saa -c UpdateBmc --file bmc.bin
OOB	./saa -i <BMC IP> -u <username> -p <password> -c UpdateBmc --file bmc.bin

The console output contains the following information.

```
Managed system..........192.168.34.56
    BMC UFFN............BMC_X13AST2600-ROT20-
D301MS_20240418_01.02.31_STDsp.bin
    BMC type............X13_RoT2.0_ATEN_AST2600_2_1
    BMC version.........01.02.31
    BMC build date.......2024/04/18
Local BMC image file.....BMC_X13AST2600-ROT20-
D301MS_20240418_01.02.31_STDsp.bin
    BMC UFFN............BMC_X13AST2600-ROT20-
D301MS_20240418_01.02.31_STDsp.bin
    BMC type............X13_RoT2.0_ATEN_AST2600_2_1
    BMC version.........01.02.31
    BMC build date.......2024/04/18
    FW image............Signed
        Signed Key.......RoT
```

```
Status: Start updating BMC for 192.168.34.56

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

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

Status: BMC is updated for 192.168.34.56

Update Complete. Please wait for BMC reboot, about 4 mins.
.................................................
.................................................
.................................................
.................................................
.................................Done
```

2. Dump NEW BMC configuration after the BMC firmware is updated.

Command Mode	Command Usage
Inband	./saa -c GetBmcCfg [--file BmcCfg.xml [--overwrite]]
OOB	./saa -i <BMC IP> -u <username> -p <password> -c GetBmcCfg [--file BmcCfg.xml [--overwrite]]

The console output contains the following information.

```
.....
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	./saa -c ChangeBmcCfg [--file BmcCfg.xml [--overwrite]]
OOB	./saa -i <BMC IP> -u <username> -p <password> -c ChangeBmcCfg [--file BmcCfg.xml]

The console output contains the following information.

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

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.

For downloading the binary BMC configuration file with the '--dump' option, there is an alternative, license-free 'DownloadBmcCfg' command available. Please refer to 5.5.3.2 Downloading BMC Configuration File for details.

For more XML details, please refer to Appendix Q. Sample Configuration Tables for BMC and CMM.



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> [--overwrite] saa -i <IP or host name> -u <username> -p <password> -c GetBmcCfg --dump --file <BmcCfg.bin> [--overwrite]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetBmcCfg [--file <BmcCfg.xml>] [--overwrite] saa -I Redfish_HI [-u <username> -p <password>] -c GetBmcCfg --dump --file <BmcCfg.bin> [--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> [--overwrite] [--remote_saa <remote SAA path>] saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetBmcCfg --

	dump --file <BmcCfg.bin> [--overwrite] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBmcCfg --file <BmcCfg.xml> [--overwrite] saa -l <system list file> [-u <username> -p <password>] -c GetBmcCfg --dump --file <BmcCfg.bin> [--overwrite]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c GetBmcCfg --file <BmcCfg.xml> [--overwrite] [--remote_saa <remote SAA path>] saa -I Remote_RHI -l <system list file> -c GetBmcCfg --dump --file <BmcCfg.bin> [--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 --
dump --file BmcCfg.bin --overwrite
```

In-Band:

```
[SAA_HOME]# ./saa -c GetBmcCfg --file BmcCfg.xml --overwrite

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetBmcCfg --dump
--file BmcCfg.bin --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 --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.56 --ou root --op 111111
-u ADMIN -p PASSWORD -c GetBmcCfg --dump --file BmcCfg.bin --overwrite --
remote_saa /root/saa
```

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 --dump -
-file BmcCfg.bin --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 --remote_saa /root/saa
```

```
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 --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetBmcCfg --dump --file
BmcCfg.bin --overwrite --remote_saa /root/saa
```

```
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 --overwrite option is used to overwrite the existing file, e.g., BmcCfg.xml.192.168.34.56 or BmcCfg.bin.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 {-I Remote_INB | -I 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
```

5.5.3.2 Downloading a BMC Configuration File

Use the “DownloadBmcCfg” command to have SAA download the current BMC configuration file from the managed system and save it in either text or binary file format by specifying the “--format” option. Both text and binary BMC configuration files are generated directly by the BMC.

The BMC configuration file in text format displays the supported and editable BMC configuration elements in XML format, while the BMC configuration file in binary format can only be used to back up and restore BMC configuration, which cannot be modified. The following shows the content of the BMC configuration file in text format.

```
<?xml version="1.0" encoding="UTF-8"?>
<IPMI>
  <Networking>
    <IPAddr value="192.168.034.056"/>
    <MacAddr value="aa:bb:cc:dd:ee:ff"/>
    <SubNetMask value="255.255.000.000"/>
    <DefaultGateWayAddr value="192.168.000.254"/>
    <DHCPEnable value="1"/>
  </Networking>
</IPMI>
```



Note:

- BMC configuration file in text format currently only supports BMC IPv4 configuration.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DownloadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml> [--overwrite]
In-Band	saa -c DownloadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml> [--overwrite]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DownloadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml> [--overwrite] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DownloadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml> [--overwrite]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DownloadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml> [--overwrite] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DownloadBmcCfg
--format BINARY --file BmcCfg.bin --overwrite

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DownloadBmcCfg
--format TEXT --file BmcCfg.xml --overwrite
```

In-Band:

```
[SAA_HOME]# ./saa -c DownloadBmcCfg --format BINARY --file BmcCfg.bin --
overwrite

[SAA_HOME]# ./saa -c DownloadBmcCfg --format TEXT --file BmcCfg.xml --
overwrite
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DownloadBmcCfg --format BINARY --file BmcCfg.bin --overwrite --
remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DownloadBmcCfg --format TEXT --file BmcCfg.xml --overwrite --
remote_saa /root/saa
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DownloadBmcCfg --
format BINARY --file BmcCfg.bin --overwrite

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DownloadBmcCfg --
format TEXT --file BmcCfg.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 DownloadBmcCfg --format
BINARY --file BmcCfg.bin --overwrite --remote_saa /root/saa
```

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c DownloadBmcCfg --format
TEXT --file BmcCfg.xml --overwrite --remote_saa /root/saa
```

```
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 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 --overwrite option is used to overwrite the existing file, e.g., BmcCfg.xml.192.168.34.56 or BmcCfg.bin.192.168.34.56.

5.5.4. Updating BMC Settings

Follow the steps below to update 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 4.7.2 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.

For uploading binary BMC configuration file with the "--restore" option, there is an alternative license-free "UploadBmcCfg" command available. Please refer to 5.5.4.1 Uploading BMC Configuration File for details.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c ChangeBmcCfg --file <BmcCfg.xml> [--skip_unknown]

	saa -i <IP or host name> -u <username> -p <password> -c ChangeBmcCfg --restore --file <BmcCfg.bin>
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c ChangeBmcCfg --file <BmcCfg.xml> [--skip_unknown] saa -I Redfish_HI -u <username> -p <password> -c ChangeBmcCfg --restore --file <BmcCfg.bin>
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> [--skip_unknown] [--remote_saa <remote SAA path>] saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c ChangeBmcCfg --restore --file <BmcCfg.bin> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeBmcCfg --file <BmcCfg.xml> [--skip_unknown] [--individually] saa -l <system list file> [-u <username> -p <password>] -c ChangeBmcCfg --restore --file <BmcCfg.bin> [--individually]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c ChangeBmcCfg --file <BmcCfg.xml> [--skip_unknown] [--individually] [--remote_saa <remote SAA path>] saa -I Remote_RHI -l <system list file> -c ChangeBmcCfg --restore --file <BmcCfg.bin> [--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 --restore --file BmcCfg.bin
```

In-Band:

```
[SAA_HOME]# ./saa -c ChangeBmcCfg --file BmcCfg.xml

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c ChangeBmcCfg --restore --file BmcCfg.bin
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c ChangeBmcCfg --file BmcCfg.xml --remote_saa /root/saa

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

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 --
restore --file BmcCfg.bin --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 --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c ChangeBmcCfg --restore --
file BmcCfg.bin --individually --remote_saa /root/saa
```

```
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.

5.5.4.1 Uploading a BMC Configuration File

1. Follow the steps in 5.5.3.2 Downloading a BMC Configuration File to download the BMC configuration file in binary or text file format.
2. a. If the configuration file is in binary format, the file is not editable and can only be used to restore BMC configuration.
   b. If the configuration file is in text format, edit the configurable element values in the BMC configuration XML file to the desired values.
3. a. If the configuration file is in binary format, use the "UploadBmcCfg" command with binary file to restore BMC configuration by specifying the "--format" option with "BINARY" value.
   b. If the configuration file is in text format, use the “UploadBmcCfg“ command with the updated XML configuration file to update the BMC configuration by specifying the "--format" option with "TEXT" value.
4. After the BMC configuration file is uploaded, the BMC will automatically reset. Please wait for BMC to boot up before proceeding with further actions.

Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c UploadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml>
In-Band	saa -c UploadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c UploadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UploadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml> [--individually]
Remote In-Band	saa -I Remote_INB -l <system list file> -c UploadBmcCfg [--format <BINARY | TEXT>] --file <BmcCfg.bin | BmcCfg.xml> [--individually] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UploadBmcCfg --format BINARY --file BmcCfg.bin

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UploadBmcCfg --format TEXT --file BmcCfg.xml
```

In-Band:

```
[SAA_HOME]# ./saa -c UploadBmcCfg --format BINARY --file BmcCfg.bin

[SAA_HOME]# ./saa -c UploadBmcCfg --format TEXT --file BmcCfg.xml
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c UploadBmcCfg --format BINARY --file BmcCfg.bin --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c UploadBmcCfg --format TEXT --file BmcCfg.xml --remote_saa /root/saa
```

Multiple Systems OOB:

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

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

```
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 UploadBmcCfg --format
BINARY --file BmcCfg.bin --individually --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c UploadBmcCfg --format
TEXT --file BmcCfg.xml --remote_saa /root/saa
```

```
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.

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	saa -l <system list file> [-u <username> -p <password>] -c SetBmcPassword [--user_id <user ID>]
Remote In-Band	saa -I Remote_INB -l < system list file> -c SetBmcPassword [--user_id <user ID>] [--remote_saa <remote SAA path>]

For Multiple Systems usage, the system list file format is fixed for the "SetBmcPassword" command, please refer to **4.4.2.4. SetBmcPassword Command**.

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 new_password
    192.168.34.57 ADMIN1 PASSWORD1 new_password
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetBmcPassword
```

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

If the execution “Status” field of the managed system shows SUCCESS, the console output of the managed system will be shown in the “Execution Message” section of the managed system in the created log file.

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 --
privi_level 'Call Back'

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetKcsPriv --
privi_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. For NVIDIA platform support, please refer to 5.5.9.1. Loading Factory BMC Settings for NVIDIA Platform.

Action / Option	Reset Network	Reset User Cfg	Reset FRU	Reset Password to
--preserve_user_cfg	N	N	N	Preserved
--clear_user_cfg with --load_default_password	N	Y	N	ADMIN
--clear_user_cfg with --load_unique_password	N	Y	N	Unique Password
--clear_user_cfg with --load_unique_password and --	Y	Y	N	Unique Password

load_default_lan				
--clear_user_cfg with --load_unique_password, --load_default_lan and --load_default_fru	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>]
Multiple Systems	
OOB	saa -l <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} -l <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.

5.5.9.1. Loading Factory BMC Settings for NVIDIA Platform

Use the “LoadDefaultBmcCfg” command to reset the NVIDIA C2 BMC and BIOS of the managed system to the factory default. The support for --reset_all option is limited to NVIDIA OpenBMC.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c LoadDefaultBmcCfg --reset_all [--bmc_boot_check [--reboot]]

In-Band	saa -I Redfish_HI -u <username> -p <password> -c LoadDefaultBmcCfg --reset_all [--reboot]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c LoadDefaultBmcCfg --reset_all [--reboot] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c LoadDefaultBmcCfg --reset_all [--bmc_boot_check [--reboot]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c LoadDefaultBmcCfg --reset_all [--reboot] [--remote_saa <remote SAA path>]

Example:

OOB:

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

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
LoadDefaultBmcCfg --reset_all --bmc_boot_check

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
LoadDefaultBmcCfg --reset_all --bmc_boot_check --reboot
```

In-Band:

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

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

Remote In-Band

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.56 --ou root --op 111111
-u ADMIN -p PASSWORD -c LoadDefaultBmcCfg --reset_all --reboot
```

Multiple OOB:

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

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg
--reset_all --bmc_boot_check

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c LoadDefaultBmcCfg
--reset_all --bmc_boot_check --reboot
```

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

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c LoadDefaultBmcCfg --
reset_all --reboot
```

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



Note:
Different NVIDIA platforms may load different configurations depending on the platform capabilities. For the NVIDIA C2 platform, the --reset_all option will load both BMC and BIOS to default settings.

5.5.10. BMC Reset

Use the “BmcReset” command to set the BMC cold or warm reset for the target system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BmcReset --action <ColdReset | WarmReset> [--bmc_boot_check]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c BmcReset --action <ColdReset | WarmReset>

	saa -c BmcReset --action <ColdReset | WarmReset> [--bmc_boot_check]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c BmcReset --action <ColdReset | WarmReset> [--bmc_boot_check]} [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcReset --action <ColdReset | WarmReset> [--bmc_boot_check]}
Remote In-Band	saa -I Remote_INB -l < system list file> -c BmcReset --action <ColdReset | WarmReset> [--bmc_boot_check]} [--remote_saa <remote SAA path>]

Example:

OOB:

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

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 BmcReset --
action WarmReset --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 BmcReset --action ColdReset
```

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

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c BmcReset --action WarmReset --remote_saa /root/saa
```

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c BmcReset --action WarmReset --bmc_boot_check --remote_saa /root/saa
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l IP_ADDR_RANGE.txt -u ADMIN -p ADMIN -c BmcReset --
bmc_boot_check --action ColdReset
```

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

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI -l IP_ADDR_RANGE.txt -c BmcReset --action
ColdReset
```

```
[SAA_HOME]# ./saa -I Remote_RHI -l IP_ADDR_RANGE.txt -c BmcReset --action
WarmReset
```

```
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 log file created for the managed system.

Note:
The --bmc_boot_check option is not supported for In-band Redfish command mode.

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 -l <system list file> [-u <username> -p <password>] -c GetBmcLANCfg [--file <BMCLANCfg.xml> [--overwrite]]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <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 [--json_view]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetBmcUserList [--json_view]
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 GetBmcUserList [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBmcUserList [--json_view]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l < system list file> -c GetBmcUserList [--json_view] [--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.
```

The console output contains the following information for Nvidia C2.

```
Maximum number of Users          : 15
Count of currently enabled Users : 1
           User Name | Privilege Level | Enabled
==================== | =============== | =======
                root |   Administrator |     Yes
==================== | =============== | =======

The BMC user list.
```

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

In-Band:

```
[SAA_HOME]# ./saa -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
======= | ==================== | =============== | =======
      2 |                ADMIN |   Administrator |     Yes
======= | ==================== | =============== | =======

The BMC user list.
```

```
[SAA_HOME]# ./saa -c GetBmcUserLis --json_viewt
```

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.
```

The console output contains the following information for Nvidia C2.

```
Maximum number of Users          : 15
Count of currently enabled Users : 1
           User Name | Privilege Level | Enabled
==================== | =============== | =======
                root |   Administrator |     Yes
==================== | =============== | =======

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 <userprivilege> [--user_status <status>] [--manage_account_type <type:status> [--ap <protocol> --pp <protocol> --ak <key> --pk <key>]] saa -i <IP or host name> -u <username> -p <password> -c SetBmcUserList --action Del {--current_user_name <current_user_name> | --user_id <userid>}

	saa -i <IP or host name> -u <username> -p <password> -c SetBmcUserList --action Level {--current_user_name <current_user_name> | --user_id <userid>} --user_privilege <userprivilege> saa -i <IP or host name> -u <username> -p <password> -c SetBmcUserList --action SetPwd {--current_user_name <current_user_name> | --user_id <userid>} --user_password <userpassword> saa -i <IP or host name> -u <username> -p <password> -c SetBmcUserList --action Test --user_name <username> --user_password <userpassword> saa -i <IP or host name> -u <username> -p <password> -c SetBmcUserList --action EnableType --user_id <userid> --account_type <type> --account_type_status <status> | --manage_account_type <type:status>} [--ap <protocol> --pp <protocol> --ak <key> --pk <key>] saa -i <IP or host name> -u <username> -p <password> -c SetBmcUserList --action EnableAccount {--current_user_name <current_user_name> | --user_id <userid>} --user_status <status> saa -i <IP or host name> -u <username> -p <password> -c SetBmcUserList --action EditUserName {--current_user_name <current_user_name> | --user_id <userid>} --user_name <username>
In-Band	saa -c SetBmcUserList --action add --user_id <userid> --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> saa -I Redfish_HI -u <username> -p <password> -c SetBmcUserList --action add [--user_id <userid>] --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> [--user_status <status>] [--manage_account_type <type:status> [--ap <protocol> --pp <protocol> --ak <key> --pk <key>]] saa -c SetBmcUserList --action Del {--user_id <userid> | -I Redfish_HI -u <username> -p <password> --current_user_name <current_user_name>} saa -c SetBmcUserList --action Level {--user_id <userid> | -I Redfish_HI -u <username> -p <password> --current_user_name <current_user_name>} --user_privilege <userprivilege> saa -c SetBmcUserList --action SetPwd {--user_id <userid> | -I Redfish_HI -u <username> -p <password> --current_user_name <current_user_name>} --user_password <userpassword>

	saa -I Redfish_HI -u <username> -p <password> -c SetBmcUserList --action Test --user_name <username> --user_password <userpassword> saa -I Redfish_HI -u <username> -p <password> -c SetBmcUserList --action EnableType --user_id {--account_type <type> --account_type_status <status> | --manage_account_type <type:status>} [--ap <protocol> --pp <protocol> --ak <key> --pk <key>] saa -c SetBmcUserList --action EnableAccount {--user_id <userid> | -I Redfish_HI -u <username> -p <password> --current_user_name <current_user_name>} --user_status <status> saa -c SetBmcUserList --action EditUserName {--user_id <userid> | -I Redfish_HI -u <username> -p <password> --current_user_name <current_user_name>} --user_name <username>
Remote In-Band	saa --oi <OS IP address> --ou <OS username> --op <OS password> -I Remote_INB -c SetBmcUserList --action add --user_id <userid> --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> saa --oi <OS IP address> --ou <OS username> --op <OS password> -I Remote_RHI -u <username> -p <password> -c SetBmcUserList --action add [--user_id <userid>] --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> [--user_status <status>] [--manage_account_type <type:status> [--ap <protocol> --pp <protocol> --ak <key> --pk <key>]] saa --oi <OS IP address> --ou <OS username> --op <OS password> -c SetBmcUserList --action Del {-I Remote_INB --user_id <userid> | -I Remote_RHI -u <username> -p <password> --current_user_name <current_user_name>} saa --oi <OS IP address> --ou <OS username> --op <OS password> -c SetBmcUserList --action Level {-I Remote_INB --user_id <userid> | -I Remote_RHI -u <username> -p <password> --current_user_name <current_user_name>} --user_privilege <userprivilege> saa --oi <OS IP address> --ou <OS username> --op <OS password> -c SetBmcUserList --action SetPwd {-I Remote_INB --user_id <userid> | -I Remote_RHI -u <username> -p <password> --current_user_name <current_user_name>} --user_password <userpassword> saa --oi <OS IP address> --ou <OS username> --op <OS password> -I Remote_RHI -u <username> -p <password> -c SetBmcUserList --action Test --user_name <username> --user_password <userpassword>

	saa --oi <OS IP address> --ou <OS username> --op <OS password> -I Remote_RHI -u <username> -p <password> -c SetBmcUserList --action EnableType --user_id {--account_type <type> --account_type_status <status> | --manage_account_type <type:status>} [--ap <protocol> --pp <protocol> --ak <key> --pk <key>] saa --oi <OS IP address> --ou <OS username> --op <OS password> -c SetBmcUserList --action EnableAccount {-I Remote_INB --user_id <userid> | -I Remote_RHI -u <username> -p <password> --current_user_name <current_user_name>} --user_status <status> saa --oi <OS IP address> --ou <OS username> --op <OS password> -c SetBmcUserList --action EditUserName {-I Remote_INB --user_id <userid> | -I Remote_RHI -u <username> -p <password> --current_user_name <current_user_name>} --user_name <username>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SetBmcUserList --action add [--user_id] <userid> --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> [--user_status <status>] [--manage_account_type <type:status> [--ap <protocol> --pp <protocol> --ak <key> --pk <key>]] saa -l < system list file > [-u <username> -p <password>] -c SetBmcUserList --action Del {--current_user_name <current_user_name> | --user_id <userid>} saa -l < system list file > [-u <username> -p <password>] -c SetBmcUserList --action Level {--current_user_name <current_user_name> | --user_id <userid>} --user_privilege <userprivilege> saa -l < system list file > [-u <username> -p <password>] -c SetBmcUserList --action SetPwd {--current_user_name <current_user_name> | --user_id <userid>} --user_password <userpassword> saa -l < system list file > [-u <username> -p <password>] -c SetBmcUserList --action Test --user_name <username> --user_password <userpassword> saa -l < system list file > [-u <username> -p <password>] -c SetBmcUserList --action EnableType --user_id <userid> --account_type <type> --account_type_status <status> | --manage_account_type <type:status>} [--ap <protocol> --pp <protocol> --ak <key> --pk <key>] saa -l < system list file > [-u <username> -p <password>] -c SetBmcUserList --action EnableAccount {--current_user_name

	<current_user_name> | --user_id <userid>} --user_status <status> saa -l < system list file > [-u <username> -p <password>] -c SetBmcUserList --action EditUserName {--current_user_name <current_user_name> | --user_id <userid>} --user_name <username>
Remote In-Band	saa -l < system list file> -I Remote_INB -c SetBmcUserList --action add --user_id <userid> --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> saa -l < system list file> -I Remote_RHI -c SetBmcUserList --action add [--user_id <userid>] --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> [--user_status <status>] [--manage_account_type <type:status> [--ap <protocol> --pp <protocol> --ak <key> --pk <key>]] saa -l < system list file> -c SetBmcUserList --action Del {-I Remote_INB --user_id <userid> | -I Remote_RHI --current_user_name <current_user_name>} saa -l < system list file> -c SetBmcUserList --action Level {-I Remote_INB --user_id <userid> | -I Remote_RHI --current_user_name <current_user_name>} --user_privilege <userprivilege> saa -l < system list file> -c SetBmcUserList --action SetPwd {-I Remote_INB --user_id <userid> | -I Remote_RHI --current_user_name <current_user_name>} --user_password <userpassword> saa -l < system list file> -I Remote_RHI -c SetBmcUserList --action Test --user_name <username> --user_password <userpassword> saa -l < system list file> -I Remote_RHI -c SetBmcUserList --action EnableType --user_id {--account_type <type> --account_type_status <status> | --manage_account_type <type:status>} [--ap <protocol> --pp <protocol> --ak <key> --pk <key>] saa -l < system list file> -c SetBmcUserList --action EnableAccount {-I Remote_INB --user_id <userid> | -I Remote_RHI --current_user_name <current_user_name>} --user_status <status> saa -l < system list file> -c SetBmcUserList --action EditUserName {-I Remote_INB --user_id <userid> | -I Remote_RHI --current_user_name <current_user_name>} --user_name <username>

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
```

OOB for Nvidia C2:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action Add --user_name NAME3 --user_password PASSWORD3 --user_privilege
3 --user_status Disable

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action Del --current_user_name CNAME3

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action Level --current_user_name CNAME3 --user_privilege 3

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action SetPwd --current_user_name CNAME3 --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 EnableAccount --current_user_name CNAME3 --user_status Disable

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetBmcUserList
--action EditUserName --current_user_name CNAME3 --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
```

In-Band through Redfish Host Interface for Nvidia C2:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 1 --user_name NAME3 --user_password PASSWORD3 --user_privilege 3 -
-user_status Disable

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 2 --current_user_name CNAME3

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 3 --current_user_name CNAME3 --user_privilege 3

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 4 --current_user_name CNAME3 --user_password PASSWORD3

[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 7 --current_user_name CNAME3 --user_status Disable

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SetBmcUserList --
action 8 --current_user_name CNAME3 --user_name NAME4
```

Multiple Systems 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
```

Multiple Systems OOB for Nvidia C2:

```
[SAA_HOME]# ./saa-l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action Add --user_name NAME3 --user_password PASSWORD3 --user_privilege 3
--user_status Disable

[SAA_HOME]# ./saa-l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action Del --current_user_name CNAME3

[SAA_HOME]# ./saa-l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action Level --current_user_name CNAME3 --user_privilege 3

[SAA_HOME]# ./saa-l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action SetPwd --current_user_name CNAME3 --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 EnableAccount --current_user_name CNAME3 --user_status Disable

[SAA_HOME]# ./saa-l SList.txt -u ADMIN -p PASSWORD -c SetBmcUserList --
action EditUserName --current_user_name CNAME3 --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
```

Multiple Systems Remote In-Band through Redfish Host Interface for Nvidia C2:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 1
--user_name NAME3 --user_password PASSWORD3 --user_privilege 3 --
user_status Disable

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 2
--current_user_name CNAME3

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 3
--current_user_name CNAME3 --user_privilege 3

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 4
--current_user_name CNAME3 --user_password PASSWORD3

[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 7
--current_user_name CNAME3 --user_status Disable

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c SetBmcUserList --action 8
--current_user_name CNAME3 --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 bootstapping account.



Notes:

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

Single System	
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c BootStrappingAccount --action <CreateAccount | DeleteAccount | CheckAccount> [--user_name <username>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c BootStrappingAccount --action <CreateAccount | DeleteAccount | CheckAccount> [--user_name <username>] [--remote_saa <remote SAA path>]
Remote In-Band Redfish Host Interface	saa -I Remote_RHI --oi <OS IP address> --ou <OS username> --op <OS password> -u <username> -p <password>-c BootStrappingAccount --action <CreateAccount | DeleteAccount | CheckAccount> [--user_name <username>] [--remote_saa <remote SAA path>]

For Multiple Systems usage, the system list file format is fixed for the “BootStrappingAccount” command, please refer to **4.4.2.6. BootStrappingAccount Command**.

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 'xxxxxxxxxxxxxx'
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c BootStrappingAccount --action 2 --user_name 'xxxxxxxxxxxxxx'
```

Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c BootStrappingAccount --action 1

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c BootStrappingAccount --action 3
```

Multiple Remote In-Band Redfish Host Interface:

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt.txt -c BootStrappingAccount --action DeleteAccount

```
SList.txt:
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD WeAoXkX5apr4lbU
    192.168.34.57 OS_Username OS_PrivateKey OS_Pvtkey_Password BMC_Username
BMC_PASSWD nVu3Zmj0aE9sSzt
```

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 -I Redfish_HI -u <username> -p <password> -c RmcpManage --action <GetInfo|Enable|Disable> [--port <port>]
Remote In-Band	saa -I Remote_RHI --oi <OS IP address> --ou <OS username> --op <OS password> -u <username> -p <password> -c RmcpManage --action <GetInfo|Enable|Disable> [--port <port>] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c RmcpManage --action <GetInfo|Enable|Disable> [--port <port>]
Remote In-Band	saa -I Remote_RHI -l <system list file> -u <username> -p <password> -c RmcpManage --action <GetInfo|Enable|Disable> [--port <port>] [--remote_saa <remote SAA path>]

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 -I Redfish_HI -u ADMIN -p PASSWORD -c RmcpManage --
action Enable --port RMCP:623
```

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 -c RmcpManage --action Enable --port RMCP:623 --
remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l Slist.txt -c RmcpManage --action
Enable --port RMCP:623
```

```
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
```

5.5.17. 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>] [--

	json_view]
In-Band	saa [-l Redfish_HI -u <username> -p <password>] -c BmcHostName --action <action> [--hostname <hostname>] [--json_view]
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 BmcHostName --action <action> [--hostname <hostname>] [--remote_saa <remote SAA path>] [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcHostName --action <action> [--json_view]
Remote In-Band	saa {-l Remote_INB | -l Remote_RHI} -l <system list file> -c BmcHostName --action <action> [--hostname <hostname>] [--remote_saa <remote SAA path>] [--json_view]

For Multiple Systems usage, the system list file format is fixed for the “BmcHostName” command, please refer to **4.4.2.5. BmcHostName Command**.

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 BmcHostName --action Get

[SAA_HOME]# ./saa -c BmcHostName --action Set --hostname 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 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 BmcHostName --action Get --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --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
```

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

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

```
SList.txt:
    192.168.34.56 testHostName
    192.168.34.57 testHostName1
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c BmcHostName --action Get
```

```
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
```

5.5.18. Managing the BMC Sessions

5.5.18.1. Getting the BMC RMCP Session Information

Use the “GetSessionInfo” command to get BMC RMCP session information.

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

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
```

5.5.18.2. Managing the BMC Redfish Sessions

Use the “SessionManage” command to manage BMC Redfish sessions.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SessionManage --action [GetInfo | Disconnect --session_id <session_id>]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c SessionManage --action [GetInfo | Disconnect --session_id <session_id>]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c SessionManage --action [GetInfo | Disconnect --session_id <session_id>] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SessionManage --action [GetInfo | Disconnect --session_id <session_id>]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c SessionManage --action [GetInfo | Disconnect --session_id <session_id>] [--remote_saa <remote SAA path>]

Example:

OOB:

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

The console output contains the following information.

```
Managed system.............................192.168.34.56
    Session service enabled...............True
    Session timeout.......................1800
    Number of currently active sessions...2
    Session ID............................1
        User Name.........................ADMIN
    Session ID............................2
        User Name.........................USER
```

In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c SessionManage --
action Disconnect --session_id 1
```

The console output contains the following information.

```
Session 1 is disconnected.
```

Multiple Systems OOB:

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

```
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>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -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>]
Remote In-Band	saa -I Remote_INB -l <system list file> -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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c ManageRHI --action 1

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c ManageRHI --action 2 --type RNDIS
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l IP_ADDR_RANGE.txt -c ManageRHI --
action 1
```

```
IP_ADDR_RANGE.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
```

5.5.20 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	saa -i <IP or host name> -u <username> -p <password> -c BmcWatchDog --action Set --timer_action <BmcWatchDog timer actions> --interval <time interval> --countdown <BmcWatchDog count down> saa -i <IP or host name> -u <username> -p <password> -c BmcWatchDog --action <Info | Reset>
In-Band	saa -c BmcWatchDog --action Set --timer_action <BmcWatchDog timer actions> --interval <time interval> --countdown <BmcWatchDog count down> saa -c BmcWatchDog --action <Info | Reset>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c BmcWatchDog --action Set --timer_action <BmcWatchDog timer actions> --interval <time interval> --countdown <BmcWatchDog count down> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcWatchDog --action Set --timer_action <BmcWatchDog timer actions> --interval <time interval> --countdown <BmcWatchDog count down> saa -l <system list file> [-u <username> -p <password>] -c BmcWatchDog --action <Info | Reset>
Remote In-Band	saa -I Remote_INB -l <system list file> -c BmcWatchDog --action <Info | Reset> [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c BmcWatchDog --action info
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p ADMIN -c BmcWatchDog --action
set --timer_action 2 --interval 10 --countdown 60
```

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

```
[SAA_HOME]# ./saa -l IP_ADDR_RANGE.txt -u ADMIN -p ADMIN -c BmcWatchDog -
-action reset
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l IP_ADDR_RANGE.txt -c BmcWatchDog --
action set --timer_action 0 --interval 10 --countdown 60
```

```
IP_ADDR_RANGE.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
```



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) Trap 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) Trap 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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SNMPManage --action GetStatus [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SNMPManage --action GetStatus
Remote In-Band	saa -I Remote_INB -l <system list file> -c SNMPManage --action GetStatus [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c SNMPManage --action GetStatus --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SNMPManage --action
GetStatus --remote_saa /root/saa
```

```
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.

5.5.21.2 Enabling Simple Network Management Protocol Trap Acknowledgement

Use the SNMPManage command with option --action On to enable Simple Network Management Protocol (SNMP) Trap acknowledgement.

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>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SNMPManage --action On --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>] [--remote_saa <remote SAA path>]
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>]
Remote In-Band	saa -I Remote_INB -l <system list file> -c SNMPManage --action On --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SNMPManage --
action On --snmp_id 1 --snmp_ip 192.168.34.58 --snmp_mac
12:34:56:78:9A:BC
```

In-Band:

```
[SAA_HOME]# ./saa -c SNMPManage --action On --snmp_id 1 --snmp_ip
192.168.34.58 --snmp_mac 12:34:56:78:9A:BC
```

The console output contains the following information.

```
Done
Seq           IP                  MAC    Acknowledge
---           --                  ---    -----------
 1 192.168.34.58    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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c SNMPManage --action On --snmp_id <snmp id> --snmp_ip <snmp ip> --snmp_mac <snmp mac> --remote_saa /root/saa
```

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SNMPManage --action On --snmp_id <snmp id> --snmp_ip <snmp ip> --snmp_mac <snmp mac> --remote_saa /root/saa
```

```
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.

5.5.21.3 Disabling Simple Network Management Protocol Trap Acknowledgement

Use the SNMPManage command with option --action Off to disable Simple Network Management Protocol (SNMP) Trap acknowledgement.

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>]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SNMPManage --action Off --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>] [--remote_saa <remote SAA path>]
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>]
Remote In-Band	saa -I Remote_INB -l <system list file> -c SNMPManage --action Off --snmp_id <snmp id> --snmp_ip <snmp ip> [--snmp_mac <snmp mac>] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SNMPManage --
action Off --snmp_id 1 --snmp_ip 192.168.34.58 --snmp_mac
12:34:56:78:9A:BC
```

In-Band:

```
[SAA_HOME]# ./saa -c SNMPManage --action Off --snmp_id 1 --snmp_ip
192.168.34.58 --snmp_mac 12:34:56:78:9A:BC
```

The console output contains the following information.

```
Done
Seq           IP                  MAC    Acknowledge
---           --                  ---    -----------
 1 192.168.34.58    12:34:56:78:9A:BC            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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c SNMPManage --action Off --snmp_id <snmp id> --snmp_ip <snmp ip> --
snmp_mac <snmp mac> --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SNMPManage --action Off --snmp_id <snmp id> --snmp_ip <snmp ip> --snmp_mac <snmp mac> --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SNMPManage --action GetCommunityString [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SNMPManage --action GetCommunityString
Remote In-Band	saa -I Remote_INB -l <system list file> -c SNMPManage --action GetCommunityString [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c SNMPManage --action GetCommunityString --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SNMPManage --action
GetCommunityString --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SNMPManage --action SetCommunityString --community_string <community_string> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SNMPManage --action SetCommunityString --community_string <community_string>
Remote In-Band	saa -I Remote_INB -l <system list file> -c SNMPManage --action SetCommunityString --community_string <community_string> [--remote_saa <remote SAA path>]

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>
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c SNMPManage --action SetCommunityString --community_string
<community_string> --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SNMPManage --action
SetCommunityString --community_string <community_string> --remote_saa
/root/saa
```

```
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.

5.5.22 Managing a BMC IPV6 Static Route

Use the BmcIPv6StaticRouteManage command to manage the BMC IPv6 static route. The command can be used to get or set the static route status to “Enabled" or "Disabled,” and it can also be used to set the static route or display the corresponding results.

- **Getting BMC IPv6 Static Route Information**
  Use the BmcIPv6StaticRouteManage command wtih the --action GetInfo option to retrive the settings of the static route.

- **Changing BMC IPv6 Static Route Status**
  Use the BmcIPv6StaticRouteManage command wtih the --action Enable option action or the --action Disable option to change the status of the static route.

- **Setting BMC IPv6 Static Route**
  Use the BmcIPv6StaticRouteManage command wtih the --action SetIPv6IP, --ipv6_ip, --ipv6_prefix_value, --ipv6_prefix_len, and --router_id options to set the IPv6 static route.

- **Clearing BMC IPv6 Static Route**
  Use the BmcIPv6StaticRouteManage command wtih the --action Clear and --router_id options to clear the IPv6 static route settings.



Note: The --router_id option has a value of 1 or 2 to specify the router.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BmcIPv6StaticRouteManage --action <action> [--router_id <Router ID> [--ipv6_ip <IPv6 IP> --ipv6_prefix_value <IPv6 prefix value> --ipv6_prefix_len <IPv6 prefix length>]]
In-Band	saa -c BmcIPv6StaticRouteManage --action <action> [--router_id <Router ID> [--ipv6_ip <IPv6 IP> --ipv6_prefix_value <IPv6 prefix value> --ipv6_prefix_len <IPv6 prefix length>]]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> [--remote_saa &<remote SAA path>] -c BmcIPv6StaticRouteManage --action <action> [--router_id <Router ID> [--ipv6_ip <IPv6 IP> --ipv6_prefix_value <IPv6 prefix value> --ipv6_prefix_len <IPv6 prefix length>]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c BmcIPv6StaticRouteManage --action <action> [--router_id <Router ID> [--ipv6_ip <IPv6 IP> --ipv6_prefix_value <IPv6 prefix value> --ipv6_prefix_len <IPv6 prefix length>]]
Remote In-Band	saa -I Remote_INB -l <system list file> [--remote_saa <remote SAA path>] -c BmcIPv6StaticRouteManage --action <action> [--router_id <Router ID> [--ipv6_ip <IPv6 IP> --ipv6_prefix_value <IPv6 prefix value> --ipv6_prefix_len <IPv6 prefix length>]]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BmcIPv6StaticRouteManage --action GetInfo
```

The console output contains the following information.

```
Managed system..............localhost
Status.....................Disabled
    Route 1
        Prefix to Route.......ABCD:0000:0000:0000:0000:0000:0000:0000/64
        Router Address........ABCD:0000:0000:0000:0000:0000:1234:5678
    Route 2
        Prefix to Route.......0000:0000:0000:0000:0000:0000:0000:0000/255
        Router Address........0000:0000:0000:0000:0000:0000:0000:0000
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BmcIPv6StaticRouteManage --action Enable
```

In-band:

```
[SAA_HOME]# ./saa -c BmcIPv6StaticRouteManage --action SetStaticRoute --
ipv6_ip 1111:2222::CCCC --ipv6_prefix_value AAAA:BBBB:: --ipv6_prefix_len
64 --router_id 2
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
BmcIPv6StaticRouteManage --action Clear --router_id 2
```

```
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. 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] | [--year | --month | --day] [--mfg] [--raw_data] [--redfish] [--file <EventLog.txt> [--overwrite]] | [--format CSV --file <EventLog.txt> [--overwrite]]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetEventLog [--info] | [--year | --month | --day] [--mfg] [--raw_data] [--file <EventLog.txt> [--overwrite]] | [--format CSV --file <EventLog.txt> [--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 GetEventLog [--info] | [--year | --month | --day] [--mfg] [--raw_data] [--file <EventLog.txt> [--overwrite]] | [--format CSV --file <EventLog.txt> [--overwrite]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetEventLog [--info] | [--year | --month | --day] [--mfg] [--raw_data] [--redfish] [--file <EventLog.txt> [--overwrite]] | [--format CSV --file <EventLog.txt> [--overwrite]]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c GetEventLog [--info] | [--year | --month | --day] [--mfg] [--raw_data] [--file <EventLog.txt> [--overwrite]] | [--format CSV --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 |  2024-03-30T19:14:05Z |         OEM |        OK | [LAN-0005] Dedicated
LAN Link Up - Assert
     2 |  2024-03-30T19:16:39Z |         OEM |        OK | [LAN-0003] System NIC
(1) Link Up - Assert
     3 |  2024-03-30T19:34:57Z |         OEM |        OK | [LAN-0003] System NIC
(1) Link Up - Assert
     4 |  2024-03-30T19:34:57Z |         OEM |   Warning | [LAN-0004] System NIC
(2) Link Down - Assert
     5 |  2024-03-30T19:40:44Z |         OEM |        OK | [LAN-0005] Dedicated
LAN Link Up - Assert
```

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

Remote In-band:

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c GetEventLog --file log.txt --remote_saa /root/saa

[SAA HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c GetEventLog --info --remote_saa /root/saa

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c GetEventLog --file log.txt --remote_saa /root/saa
```

```
[SAA HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c GetEventLog --file log --format csv --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetEventLog --raw_data --
remote_saa /root/saa
```

```
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 GetEventLog --file log --
format csv --overwrite--remote_saa /root/saa
```

```
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 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]
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 ClearEventLog [--current_password <current password> | --cur_pw_file <current password file path>] [--reboot] [--clear_bmc_eventlog] [--clear_bios_eventlog]
Multiple Systems	
OOB	saa -l <system list file> -u [<username> -p <password>] -c ClearEventLog [--reboot [--post_complete]] [--clear_bmc_eventlog] [--clear_bios_eventlog]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c ClearEventLog [--reboot] [--clear_bmc_eventlog] [--clear_bios_eventlog]

For Multiple Systems usage, the managed systems should be enumerated row by row in the system list file. For the “ClearEventLog” command, the system list file format is fixed for specific commands. Please refer to 5.4.3. Getting Current BIOS Settings. If the command is executed under pure Redfish mode, the Current_BIOS_Password field is no needed and should be removed from the system list.

Example:

OOB:

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

In-Band:

```
[SAA_HOME]# ./saa -c ClearEventLog --clear_bmc_eventlog --reboot
```

Remote In-Band:

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

In-Band Redfish Host Interface:

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

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p ADMIN -c ClearEventLog --
clear_bios_eventlog --reboot
```

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

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ClearEventLog --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
```

Multiple Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c ClearEventLog --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
```

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]] [--json_view]
In-Band	saa -c GetMaintenEventLog [--st <start time> --et <end time>] [--count <log count>] [--file < MaintenEventLog.txt> [--overwrite]] [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetMaintenEventLog [--st <start time> --et <end time>] [--count <log count>] [--file < MaintenEventLog.txt> [--overwrite]] [--json_view] [--remote_saa <remote SAA path>]
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]] [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetMaintenEventLog [--st <start time> --et <end time>] [--count <log count>] [--file < MaintenEventLog.txt> [--overwrite]] [--json_view] [--remote_saa <remote SAA path>]

Example:

OOB:

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

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

In-Band:

```
[SAA_HOME]# ./saa -c GetMaintenEventLog --file MaintenEventLog.txt --
overwrite

[SAA_HOME]# ./saa -c GetMaintenEventLog --file MaintenEventLog.txt --
overwrite --json_view
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c GetMaintenEventLog --file MaintenEventLog.txt --overwrite --remote_saa
/root/saa
```

Multiple OOB:

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

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetMaintenEventLog --file
MaintenEventLog.txt --overwrite
```

```
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
```

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 AMD 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 -I Redfish_HI -u <username> -p <password> -c GetHostDump --action <actiondump> [--file <HostDump.tgz> [--overwrite]]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetHostDump --action <actiondump> [--file <HostDump.tgz> [--overwrite]] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetHostDump --action <actiondump> [--file <HostDump.tgz> [--overwrite]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetHostDump --action <actiondump> [--file <HostDump.tgz> [--overwrite]] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p ADMIN -c GetHostDump --
action 1 --file log.tgz

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p ADMIN -c GetHostDump --
action 2

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p ADMIN -c GetHostDump --
action 3 --file log.tgz
```

In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p ADMIN -c GetHostDump --action
1 --file log.tgz
```

Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c GetHostDump --action 3 --file log.tgz --remote_saa
/root/saa
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l IP_ADDR_RANGE.txt -u ADMIN -p ADMIN -c GetHostDump -
-action CreateDump --file log.tgz --overwrite
```

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

Multiple Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l IP_ADDR_RANGE.txt -c GetHostDump --
action 2
```

```
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
```

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]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c ClearMaintenEventLog [--gen_log] [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c ClearMaintenEventLog [--gen_log]
Remote In-Band	saa -I Remote_INB -l <system list file> -c ClearMaintenEventLog [--gen_log] [--remote_saa <remote SAA path>]

Example:

OOB:

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

In-Band:

```
[SAA_HOME]# ./saa -c ClearMaintenEventLog --gen_log
```

Remote In-Band:

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

Multiple Systems OOB:

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

```
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.

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ClearMaintenEventLog
```

```
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
```

5.6.6. Setting SEL Time Mode

Use the “SetSELTimeMode” command to execute SAA to set the SEL time of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SetSELTimeMode --time <time>
In-Band	saa -c SetSELTimeMode --time <time>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SetSELTimeMode --time <time>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SetSELTimeMode --time <time>
Remote In-Band	saa -I Remote_INB -l <system list file> -c SetSELTimeMode --time <time>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c SetSELTimeMode
--time 20240716120000
```

In-Band:

```
[SAA_HOME]# ./saa -c SetSELTimeMode --time 202407161200
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c SetSELTimeMode --time 20240716120000 --remote_saa /root/saa
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SetSELTimeMode --
time 20240716120000
```

```
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 SetSELTimeMode --time
202407161200--remote_saa /root/saa
```

```
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 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>] [--showall] [--json_view]
In-Band	saa -c GetCmmInfo --file <filename> --file_only [--json_view]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetCmmInfo [--file <filename>] [--showall] [--json_view]

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 "--showall" option.

```
Blade ID: B6
==============
Node ID: 1
    Board model.........BH12SSi
    Status..............Normal
    BMC IP..............192.168.34.57
    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.

- 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.

For more XML details, please refer to **Appendix Q. Sample Configuration Tables** for BMC and CMM.



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:

OOB:

```
[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 OOB:

```
[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	saa -i <IP or host name> -u <username> -p <password> -c ChangeCmmCfg --file <CmmCfg.xml> [--skip_unknown] [--precheck] saa -i <IP or host name> -u <username> -p <password> -c

	ChangeCmmCfg {--upload --file <CmmCfg.xml> [--skip_precheck] | --update Apply | Deploy [--skip_unknown] [--precheck]}
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeCmmCfg --file <CMMCfg.xml> [--skip_unknown] [--precheck] [--individually] saa -i <system list file> [-u <username> -p <password>] -c ChangeCmmCfg {--upload --file <CmmCfg.xml> [--skip_precheck] | --update Apply | Deploy [--skip_unknown] [--precheck]}

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” udpates CMM immediately with a CMM profile.
- For immediate update, if the scheduled update time in CMM profile expires, CMM configuration will be updated immediately.
- For scheduled updates, if the scheduled update time in CMM profile is in the future, CMM configuration will be updated at the scheduled update time.
- For 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_password	N	Y	N	**ADMIN**
--clear_user_cfg with --load_unique_password	N	Y	N	**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>] [--json_view]
In-Band	saa -c GetBbpInfo [--file_only <filename>] [--json_view]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetBbpInfo [--file <filename>] [--json_view]

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

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:

OOB:

```
[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. 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

5.7.12.1. 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 [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action GetBladePsuInfo [--json_view]

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.

5.7.12.2. 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 [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action GetBladePsuConsumption [--json_view]

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.

5.7.12.3. 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 [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action GetFanSpeed [--json_view]

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.

5.7.12.4. 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> [--json_view]

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action SetFanSpeed --value <value> [--json_view]

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.

5.7.12.5. Getting Blade System Fan Mode

Use the BladePsuManage command with option --action GetFanMode to get Blade system fan mode from managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladePsuManage --action GetFanMode [--json_view]
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action GetFanMode [--json_view]

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.

5.7.12.6. 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> [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladePsuManage --action SetFanMode --value <value> [--json_view]

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.

5.7.13 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	• Gets and edits profile information or deletes the profile on CMM • Provides profile association information between specified profile and the selected Blade systems.
GetCmmCfg	Downloads the current repository CMM configuration from CMM.
ChangeCmmCfg	• Uploads the CMM configuration to CMM. • Updates the CMM configuration to CMM by the existing CMM configuration on CMM.
GetSystemCfg	Downloads the current or repository system configuration from CMM.
ChangeSystemCfg	• Uploads the CMM configuration to CMM. • Updates the system configuration to a Blade system through CMM with the existing system configuration on CMM.

5.7.13.1 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.

5.7.13.2. 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.

5.7.13.3. 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.

5.7.13.4. 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.

5.7.14 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 [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeSummary [--json_view]

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 OOB:

```
[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.

5.7.15 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 [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetCmmUserList [--json_view]

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.
```

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

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.

5.7.16 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	saa -i <IP or host name> -u <username> -p <password> -c SetCmmUserList --action add --user_id <userid> --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> saa -i <IP or host name> -u <username> -p <password> -c SetCmmUserList --action <action> --user_id <userid> [--user_name <username>] [--user_password <userpassword>] [--user_privilege <userprivilege>] saa -i <IP or host name> -u <username> -p <password> -c SetCmmUserList --action Test --user_name <username> --user_password <userpassword> saa -i <IP or host name> -u <username> -p <password> -c SetCmmUserList --action EnableType --user_id --account_type <type> --account_type_status <status> [--ap <protocol> --pp <protocol> --ak <key> --pk <key>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SetCmmUserList --action add --user_id <userid> --user_name <username> --user_password <userpassword> --user_privilege <userprivilege> saa -l < system list file > [-u <username> -p <password>] -c SetCmmUserList --action <action> --user_id <userid> [--user_name <username>] [--user_password <userpassword>] [--user_privilege <userprivilege>] saa -l < system list file > [-u <username> -p <password>] -c

	SetCmmUserList --action Test --user_name <username> --user_password <userpassword> saa -l < system list file > [-u <username> -p <password>] -c SetCmmUserList --action EnableType --user_id --account_type <type> --account_type_status <status> [--ap <protocol> --pp <protocol> --ak <key> --pk <key>]

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 Systems 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.

5.7.17 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
```

5.7.18 Launching Blade Console

Use the “BladeConsole” command to launch a remote blade console within CMM based on the specified blade ID and node ID.



Note:
You can use BladeSummary command to check Blade ID and Node ID within CMM..

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeConsole --blade_id <blade ID> --node_id <node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c BladeConsole --blade_id A1 --node_id 1
```

5.7.19 Managing Nodes within the Blade System

Use the "BladeNodeManage" command to manage the nodes of the Blade system through the CMM.

The following table summarizes the supported actions in BladeNodeManage command.

Option	--action
Description	GetSensor = Gets Blade node sensor GetStatus = Gets Blade node status GetPower = Gets Blade node power SetPower = Sets Blade node power GetIp = Gets Blade node IP SetIp = Sets Blade node IP GetDhcp = Gets Blade node DHCP SetDhcp = Sets Blade node DHCP GetMac = Gets Blade node MAC SetMac = Sets Blade node MAC GetMask = Gets Blade node mask SetMask = Sets Blade node mask GetGateway = Gets Blade node gateway SetGateway = Sets Blade node gateway GetName = Gets Blade node name SetName = Sets Blade node name GetUid = Gets Blade node UID SetUid = Sets Blade node UID GetSystemModel = Gets Blade node system model

5.7.19.1 Getting Blade Node Sensor

Use the BladeNodeManage command with the --action GetSensor option to get the sensor status of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetSensor [--blade_id <Blade ID> [--node_id <Node ID>]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetSensor [--blade_id <Blade ID> [--node_id <Node ID>]]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetSensor --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Status          | Name              | Reading      | Low CT   | High CT
--------------- | ---------------   | ------------ | -------- | --------
Normal          | CPU Temp          | 54°C         | 0°C      | 107°C
N/A             | Inlet Temp        | N/A          | N/A      | N/A
Normal          | System Temp       | 39°C         | 0°C      | 85°C
Normal          | Peripheral Temp   | 43°C         | 0°C      | 85°C
Normal          | CPU_VRMIN Temp    | 54°C         | 0°C      | 100°C
Normal          | CPU_VRMHV Temp    | 42°C         | 0°C      | 100°C
Normal          | CPU_VRMON Temp    | 52°C         | 0°C      | 100°C
N/A             | Hotswap1 VOUT     | N/A          | N/A      | N/A
N/A             | Hotswap1 IOUT     | N/A          | N/A      | N/A
N/A             | Hotswap1 Temp     | N/A          | N/A      | N/A
N/A             | Hotswap1 Status   | N/A          | N/A      | N/A
N/A             | Hotswap2 VOUT     | N/A          | N/A      | N/A
N/A             | Hotswap2 IOUT     | N/A          | N/A      | N/A
N/A             | Hotswap2 Temp     | N/A          | N/A      | N/A
N/A             | Hotswap2 Status   | N/A          | N/A      | N/A
Normal          | Hotswap Temp      | 42°C         | 0°C      | 95°C
N/A             | U2_SSD Temp       | N/A          | N/A      | N/A
Normal          | MB 12V            | 12.309 V     | 10.779 V | 13.209 V
Normal          | MB 5VCC           | 5.03 V       | 4.484 V  | 5.534 V
```

```
Normal          | MB 3.3VCC         | 3.32 V       | 2.958 V  | 3.633 V
Normal          | VBAT              | presence     | N/A      | N/A
Normal          | MB 5V_AUX         | 4.987 V      | 4.484 V  | 5.534 V
Normal          | MB 3.3V_AUX       | 3.296 V      | 2.958 V  | 3.633 V
Normal          | CPU_PVNN          | 1.007 V      | 0.831 V  | 1.173 V
N/A             | HDD Temp          | N/A          | N/A      | N/A
N/A             | NIC Temp          | N/A          | N/A      | N/A
N/A             | P1_DIMMA~F Temp   | N/A          | N/A      | N/A
N/A             | VCPU1_VCCIN       | N/A          | N/A      | N/A
N/A             | VCPU1_VCCON       | N/A          | N/A      | N/A
N/A             | VCPU1_VCCEHV      | N/A          | N/A      | N/A
N/A             | P1_DIMMG~L Temp   | N/A          | N/A      | N/A
N/A             | VCPU1_VCCFIV      | N/A          | N/A      | N/A
N/A             | VCPU1_VCCHV       | N/A          | N/A      | N/A
N/A             | Watchdog          | N/A          | N/A      | N/A
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetSensor --blade_id A1 --node_id 1
```

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

5.7.19.2 Getting Blade Node Status

Use the BladeNodeManage command with the --action GetStatus option to get the status of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetStatus [--blade_id <Blade ID> [--node_id <Node ID>]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetStatus [--blade_id <Blade ID> [--node_id <Node ID>]]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetStatus --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Item                          |                Value
----                          |                -----
Location                      |      Blade A1 Node 1
Model Name                    |        B14SBE-CPU-AP
Blade Max Power               |                 661
Blade Current Power           |                 100
Error                         |              Normal
Post Code                     |                  00
BMC Version                   |            1.02.05
BMC IP Address                |       192.168.34.56
BMC MAC                       |    12:34:56:78:9A:BC
KVM                           |         Not Launched
Blade UID                     |             Disabled
Name                          |
Power Status                  |                  On
BIOS ID                       |        B14SBE-CPU-AP
BIOS Version                  |                 1.1
BIOS Build Date               |           03/17/2025
Num of CPU                    |                   1
CPU ID                        |                1745
CPU Speed                     |             2700 MHz
Num of DIMM                   |                   1
Memory Size                   |             32.0 GB
Memory Speed                  |             4800 MHz
Num of NIC                    |                   1
NIC1 MAC                      |    12:34:56:78:9A:BD
NIC2 MAC                      |    12:34:56:78:9A:BE
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetStatus --blade_id A1 --node_id 1
```

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

5.7.19.3 Getting Blade Node Power

Use the BladeNodeManage command with the --action GetPower option to get the power status of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetPower --blade_id <Blade ID> --node_id <Node ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetPower --blade_id <Blade ID> --node_id <Node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetPower --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1 is currently powered on.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetPower --blade_id A1 --node_id 1
```

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

5.7.19.4 Setting Blade Node Power

Use the BladeNodeManage command with the --action SetPower option to set the power status of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action SetPower --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action SetPower --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action SetPower --blade_id A1 --node_id 1 --value 1
```

The console output contains the following information.

```
Blade A1 Node 1 power action is completed.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action SetPower --blade_id A1 --node_id 1 --value 1
```

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

5.7.19.5 Getting Blade Node IP Address

Use the BladeNodeManage command with the --action GetIp option to get the IP of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetIp --blade_id <Blade ID> --node_id

	<Node ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetIp --blade_id <Blade ID> --node_id <Node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetIp --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1 IP: 192.168.34.58
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetIp --blade_id A1 --node_id 1
```

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

5.7.19.6 Setting Blade Node IP Address

Use the BladeNodeManage command with the --action SetIp option to set the IP of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action SetIp --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action SetIp --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action SetIp --blade_id A1 --node_id 1 --value
192.168.34.58
```

The console output contains the following information.

```
Blade A1 Node 1 IP address setting is completed.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action SetIp --blade_id A1 --node_id 1 --value 192.168.34.58
```

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

5.7.19.7 Getting Blade Node DHCP

Use the BladeNodeManage command with the --action GetDhcp option to get the DHCP status of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetDhcp --blade_id <Blade ID> --node_id <Node ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetDhcp --blade_id <Blade ID> --node_id

	<Node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetDhcp --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1 IP mode: DHCP
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetDhcp --blade_id A1 --node_id 1
```

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

5.7.19.8 Setting Blade Node DHCP

Use the BladeNodeManage command with the --action SetDhcp option to set the DHCP of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action SetDhcp --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action SetDhcp --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action SetDhcp --blade_id A1 --node_id 1 --value 2
```

The console output contains the following information.

```
Blade A1 Node 1 IP mode setting is completed.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action SetDhcp --blade_id A1 --node_id 1 --value 2
```

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

5.7.19.9 Getting Blade Node MAC Address

Use the BladeNodeManage command with the --action GetMac option to get the MAC of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetMac --blade_id <Blade ID> --node_id <Node ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetMac --blade_id <Blade ID> --node_id <Node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetMac --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1 MAC address: 12:34:56:78:9A:BC
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetMac --blade_id A1 --node_id 1
```

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

5.7.19.10 Setting Blade Node MAC Address

Use the BladeNodeManage command with the --action SetMac option to set the MAC of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action SetMac --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action SetMac --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action SetMac --blade_id A1 --node_id 1 --value
12:34:56:78:9A:BC
```

The console output contains the following information.

```
Blade A1 Node 1 MAC address setting is completed.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action SetMac --blade_id A1 --node_id 1 --value 12:34:56:78:9A:BC
```

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

5.7.19.11 Getting Blade Node Subnet Mask

Use the BladeNodeManage command with the --action GetSubnetMask option to get the subnet mask of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetSubnetMask --blade_id <Blade ID> --node_id <Node ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetSubnetMask --blade_id <Blade ID> --node_id <Node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetSubnetMask --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1 subnet mask: 255.255.0.0
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetSubnetMask --blade_id A1 --node_id 1
```

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

5.7.19.12 Setting Blade Node Mask

Use the BladeNodeManage command with the --action SetSubnetMask option to set the subnet mask of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action SetSubnetMask --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action SetSubnetMask --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action SetSubnetMask --blade_id A1 --node_id 1 --value
255.255.0.0
```

The console output contains the following information.

```
Blade A1 Node 1 subnet mask setting is completed.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action SetSubnetMask --blade_id A1 --node_id 1 --value 255.255.0.0
```

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

5.7.19.13 Getting Blade Node Gateway

Use the BladeNodeManage command with the --action GetGateway option to get the gateway of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetGateway --blade_id <Blade ID> --node_id <Node ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetGateway --blade_id <Blade ID> --node_id <Node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetGateway --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1 gateway: 192.168.34.1
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetGateway --blade_id A1 --node_id 1
```

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

5.7.19.14 Setting Blade Node Gateway

Use the BladeNodeManage command with the --action SetGateway option to set the gateway of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action SetGateway --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action SetGateway --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action SetGateway --blade_id A1 --node_id 1 --value
192.168.34.1
```

The console output contains the following information.

```
Blade A1 Node 1 gateway setting is completed.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action SetGateway --blade_id A1 --node_id 1 --value 192.168.34.1
```

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

5.7.19.15 Getting Blade Node Name

Use the BladeNodeManage command with the --action GetName option to get the name of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetName --blade_id <Blade ID> --node_id <Node ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetName --blade_id <Blade ID> --node_id <Node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetName --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1 name: Blade-A1-Node-1
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetName --blade_id A1 --node_id 1
```

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

5.7.19.16 Setting Blade Node Name

Use the BladeNodeManage command with the --action SetName option to set the name of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action SetName --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action SetName --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action SetName --blade_id A1 --node_id 1 --value Blade-
A1-Node-1
```

The console output contains the following information.

```
Blade A1 Node 1 name setting is completed.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action SetName --blade_id A1 --node_id 1 --value Blade-A1-Node-1
```

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

5.7.19.17 Getting Blade Node UID

Use the BladeNodeManage command with the --action GetUid option to get the UID of a Blade node from the managed system.

Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetUid --blade_id <Blade ID> --node_id <Node ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetUid --blade_id <Blade ID> --node_id <Node ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetUid --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1 UID status: Off
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetUid --blade_id A1 --node_id 1
```

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

5.7.19.18 Setting Blade Node UID

Use the BladeNodeManage command with the --action SetUid option to set the UID of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action SetUid --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action SetUid --blade_id <Blade ID> --node_id <Node ID> --value <assignment value>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action SetUid --blade_id A1 --node_id 1 --value on
```

The console output contains the following information.

```
Blade A1 Node 1 UID setting is completed.
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action SetUid --blade_id A1 --node_id 1 --value on
```

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

5.7.19.19 Getting Blade Node System Model

Use the BladeNodeManage command with the --action GetSystemModel option to get the system model of a Blade node from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c BladeNodeManage --action GetSystemModel [--blade_id <Blade ID> [--node_id <Node ID>]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BladeNodeManage --action GetSystemModel [--blade_id <Blade ID> [-

	-node_id <Node ID>]]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
BladeNodeManage --action GetSystemModel --blade_id A1 --node_id 1
```

The console output contains the following information.

```
Blade A1 Node 1: ABC-123
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c BladeNodeManage --
action GetSystemModel --blade_id A1 --node_id 1
```

```
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	saa -i <IP or host name> -u <username> -p <password> -c GetRaidControllerInfo [--file <filename>] [--controller <Broadcom|Marvell>] [--dev_id <controller_id>] [--json_view]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetRaidControllerInfo [--file <filename> [--file_only]] [--controller <Broadcom|Marvell>] [--dev_id <controller_id>] [--json_view]

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetRaidControllerInfo [--file <filename> [--file_only]] [--controller <Broadcom|Marvell>] [--dev_id <controller_id>] [--json_view] [--remote_saa <remote SAA path>] saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -u <username> -p <password> -c GetRaidControllerInfo [--file <filename> [--file_only]] [--controller <Broadcom|Marvell>] [--dev_id <controller_id>] [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetRaidControllerInfo [--file <filename>] [--controller <Broadcom|Marvell>] [--dev_id <controller_id>] [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetRaidControllerInfo [--file <filename> [--file_only]] [--controller <Broadcom|Marvell>] [--dev_id <controller_id>] [--json_view] [--remote_saa <remote SAA path>] saa -I Remote_INB -l <system list file> -u <username> -p <password> -c GetRaidControllerInfo [--file <filename> [--file_only]] [--controller <Broadcom|Marvell>] [--dev_id <controller_id>] [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GetRaidControllerInfo --file RAID.rom --file_only --remote_saa
/root/saa
```

Multiple Systems 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 -c GetRaidControllerInfo --file RAID.rom --file_only
--remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetRaidControllerInfo --
file RAID.rom --file_only --remote_saa /root/saa
```

```
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 GetRaidControllerInfo --
file RAID.rom --file_only --remote_saa /root/saa
```

```
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 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 "UpdateRaidController" command with RAID firmware image file to update the managed system.



Notes:

- Supported RAID controllers:
  Broadcom: 3108, 3408, 3808, 3808N(AOM-S3808NI-4NM, AOC-SMG4-2M2, AOM-M3808NI-4HM), 3816, 3908, 3916 and 4116
  Marvell: SE9230 and 88NR2241
- Broadom 3108 RAID controller 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.
- Marvell 88NR2241 RAID controller cannot support "--upgrade_only" option since the firmware version in Marvell 88NR2241 firmware image cannot be retrieved.

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> [--upgrade_only] [{[--reboot] | [--check_reboot_required]}]
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> [--upgrade_only] [{[--reboot] | [--check_reboot_required]}]
Remote In-Band	saa -I Remote_RHI --oi <OS IP address> --ou <OS username> --op <OS password> -u <username> -p <password> -c UpdateRaidController --file <filename> --controller <Broadcom|Marvell> [--type <HBA|HA-RAID>] --dev_id <controller_id> [--upgrade_only] [{[--reboot] | [--check_reboot_required]}]
Multiple Systems	
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> [--upgrade_only] [{[--reboot] | [--check_reboot_required]}]
Remote In-Band	saa -I Remote_RHI -l <system list file> -u <username> -p <password> -c UpdateRaidController --file <filename> --controller <Broadcom|Marvell> [--type <HBA|HA-RAID>] --dev_id <controller_id> [--upgrade_only] [{[--reboot] | [--check_reboot_required]}]

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 --
upgrade_only --reboot --post_complete
```

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 -c UpdateRaidController --controller Marvell --dev_id 0 --file RAID.rom --upgrade_only --reboot --post_complete --remote_saa /root/saa
```

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 --upgrade_only --check_reboot_required
```

```
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 UpdateRaidController --controller Marvell --dev_id 0 --file RAID.rom --upgrade_only --reboot --post_complete --remote_saa /root/saa
```

```
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
```

5.8.3. 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 RAIDCfg.xml file.



Notes:

- The received tables/elements between the two managed systems might not be identical. Only the supported tables/elements for the managed system will be received.
- The 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]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetRaidCfg --file <filename> [--overwrite] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetRaidCfg --file <filename> [--overwrite]
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetRaidCfg --file <filename> [--overwrite] [--remote_saa <remote SAA path>]

Example:

OOB:

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

In-Band:

```
[SAA_HOME]# ./saa -c GetRaidCfg --file RAIDCfg.xml --overwrite
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 overwrite --remote_saa /root/saa
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetRaidCfg --file RAIDCfg.xml --overwrite
```

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

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetRaidCfg --file
RAIDCfg.xml --overwrite --remote_saa /root/saa
```

```
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 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c ChangeRaidCfg --file <filename> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeRaidCfg --file <filename>
Remote In-Band	saa -I Remote_INB -l <system list file> -c ChangeRaidCfg --file <filename> [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c ChangeRaidCfg --file RAIDCfg.xml --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c ChangeRaidCfg --file
RAIDCfg.xml --remote_saa /root/saa
```

```
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 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>] [--redfish]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetNvmeInfo [--dev_id <device_id>] saa -c GetNvmeInfo [--dev_id <device_id>]
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 GetNvmeInfo [--dev_id <device_id>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetNvmeInfo [--dev_id <device_id>]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c GetNvmeInfo [--dev_id <device_id>]

Example:

In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GetNvmeInfo --
dev_id 0
```

The console output contains the following information.

```
NVMe Device information
=======================
    [NVMe Controller(1)]
        [Group(1)]
            Group ID: 0
            [NVMe SSD(1)]
                Name: Disk.Bay.1
                Manufacturer: Samsung
                Model Number: SAMSUNG MZ3LO1T9HCJR-00A07
```

```
                Serial Number: S79JNG0X102271
                Capacity Bytes: 1920383410176
                Capable SpeedGbs: 126.000000
                Percecntage Drive Life Used: 0
                Drive Functional: true
                Temperature: 26 degree C
                Failure Predicted: false
                Status Indicator: OK
```

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: S1NONYAF800079
                Model Number: MZWEI400HAGM-0003
                Port 0 Max Link Speed: 8 GT/s
                Port 0 Max Link Width: x4
                Port 1 Max Link Speed: N/A
                Port 1 Max Link Width: N/A
                Initial Power Requirement: 10 Watts
                Max Power Requirement: 25 Watts
                Located Status: Not Located
```

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: S1NONYAF800079
                Model Number: MZWEI400HAGM-0003
                Port 0 Max Link Speed: 8 GT/s
                Port 0 Max Link Width: x4
                Port 1 Max Link Speed: N/A
                Port 1 Max Link Width: N/A
                Initial Power Requirement: 10 Watts
                Max Power Requirement: 25 Watts
                Located Status: Not Located
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c GetNvmeInfo --dev_id 0 --remote_saa /root/saa
```

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

Multiple Systems OOB:

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

```
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 GetNvmeInfo --dev_id 0 --
remote_saa /root/saa
```

```
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 GetNvmeInfo --dev_id 0 --
remote_saa /root/saa
```

```
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 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>] [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetPMemInfo [--file <filename>] [--json_view] saa -c GetPMemInfo --file <filename> --file_only [--json_view]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetPMemInfo [--file <filename>] [--json_view]

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 -c GetPMemInfo --file PMem.bin --file_only
```

In-Band Redfish Host Interface:

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

Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c GetPMemInfo --file PMem.bin
```

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
```

Multiple Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetPMemInfo --file
PMem.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.



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 -I 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]
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 UpdatePMem --file <filename> [--reboot] saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -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} [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c UpdatePMem --file <filename> [--reboot] saa -I Remote_INB -l <system list file> -c UpdatePMem --restore_default_fw [--reboot]

For Multiple Systems usage, the managed systems should be enumerated row by row in the system list file. For the “UpdatePMem” command with option --restore_default_fw, the system list file format is fixed for specific commands. Please refer to 5.4.3. Getting Current BIOS Settings. If the command is executed with option --file, the Current_BIOS_Password field is no needed and should be removed from the system list.

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.
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c UpdatePMem --restore_default_fw --reboot
```

Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c UpdatePMem --file PMem.bin --reboot
```

Multiple Systems OOB:

```
[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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c UpdatePMem --
restore_default_fw --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
```

Multiple Remote In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c UpdatePMem --file
PMem.bin --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
```

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 <VROC.cfg.xml> [--overwrite]

In-Band	saa -I Redfish_RHI -u <username> -p <password> -c GetVROCCfg --file <VROC.cfg.xml> [--overwrite]
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 GetVROCCfg --file <VROC.cfg.xml> [--overwrite]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetVROCCfg --file <VROC.cfg.xml> [--overwrite]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c GetVROCCfg --file <VROC.cfg.xml> [--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 -I Redfish_HI -u ADMIN -p PASSWORD -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 <VROC.cfg.xml>
In-Band	saa -I Redfish_RHI -u <username> -p <password> -c ChangeVROCCfg --file <VROC.cfg.xml>
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 ChangeVROCCfg --file <VROC.cfg.xml>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeVROCCfg --file <VROC.cfg.xml>
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c ChangeVROCCfg --file <VROC.cfg.xml>

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 -I Redfish_HI -u ADMIN -p PASSWORD -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 Informantion for details. This command supports four actions:

- **Locate:** locates the device by turning on its LED light.

- **StopLocate:** stops locating the device by turning off its LED light.
- **Insert:** inserts the device.
- **Remove:** removes the device.
- **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>
Multiple Systems	
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 –- deveice_name <DEVICE_NAME>
In-Band	saa -c GetSmartData --deveice_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>] [--json_view]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetSasExpanderInfo [--file <filename> [--file_only]] [--json_view]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c

	GetSasExpanderInfo [--file <filename>] [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetSasExpanderInfo [--file <filename>] [--json_view]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetSasExpanderInfo [--file <filename>] [--remote_saa <remote SAA path>] [--json_view]

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 <index> [--reboot]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateSasExpander --file <filename> --index <index> [--reboot]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateSasExpander --file <filename> -index <index> [--reboot] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateSasExpander --file <filename> --index <index> [--reboot]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c UpdateSasExpander --file <filename> -index <index> [--reboot] [--remote_saa <remote SAA path>]

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 [--json_view]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetPsuInfo [--json_view]
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 GetPsuInfo [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> -u <username> -p <password> -c GetPsuInfo [--json_view]

Remote In-Band	saa {-I Remote_INB | -I Remote_RHI>} -l <system list file> -c GetPsuInfo [--json_view] [--remote_saa <remote SAA path>]

Example:

OOB:

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

In-Band:

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

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

The console output contains the following information.

Note that the console output may vary when getting PSU info through different interface, depending on the BMC version.

Getting PSU information throught Redfish:

```
[Module 1]:
    PWS Module Number: PWS-2K07A-1R
    PWS Serial Number: P2K7ACN32PB0126
    PWS Module Revision: 1.0
    Firmware Version: 1.0
    Status: OK
    AC Input Voltage: 116 V
    AC Input Current: 0.94 A
    DC 12V Output Voltage: 12.10 V
    DC 12V Output Current: 7.04 A
    Temperature 1: 40 C / 104 F
    Temperature 2: 62 C / 144 F
    Fan 1: 12448 RPM
    Fan 2: 0 RPM
    DC 12V Output Power: 85 W
    AC Input Power: 108 W
    Current Sharing Control: Active
```

Getting PSU information throught PMBus:

```
[Module 1](SlaveAddress = 0xB0)
    PWS Module Number: PWS-2K09A-1R
```

```
    PWS Serial Number: P2K09CN53IB0413
    PWS Module Revision: 1.0
    PMBus Revision: 0x22
    Status: OK
    AC Input Voltage: 114.00 V
    AC Input Current: 0.98 A
    DC 12V Output Voltage: 12.15 V
    DC 12V Output Current: 7.38 A
    Temperature 1: 34 C / 93 F
    Temperature 2: 56 C / 133 F
    Fan 1: 6048 RPM
    Fan 2: 0 RPM
    DC 12V Output Power: 89 W
    AC Input Power: 111 W
    Current Sharing Control: Active - Active (90)
```

Remote In-Band:

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

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetPsuInfo
```

```
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 GetPsuInfo
```

```
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 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 the signed PSU firmware image required by the OEM and specify the PSU index or slave address to execute SAA to update the managed system.



Notes:

- The target system must be powered off while updating PSU firmware.
- The "--index all" option can be used to update all PSUs on the system; however, all PSUs must be of the same PSU model and PSU hardware version.
- The "--index" option can be used without the "--file" option, provided that the PSU firmware image is placed in the designated directory within SAA. Example: <SAApath>/<PSU model name>/<PSU HW revision>/<PSU firmware image>
- The "--reboot" and "--post_complete" options are only supported when using the option "--index".

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdatePsu --file <filename> --address <PSU slave address> saa -i <IP or host name> -u <username> -p <password> -c UpdatePsu [--file <filename>] --index <PSU index> --reboot [--post_complete]
In-Band	saa -c UpdatePsu --file <filename> --address <PSU slave address>

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdatePsu --file <filename> --address <PSU slave address> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdatePsu --file <filename> --address <PSU slave address> saa -l <system list file> [-u <username> -p <password>] -c UpdatePsu --file [<filename>] --index <PSU index> --reboot [--post_complete]
Remote In-Band	saa -I Remote_INB -l <system list file> -c UpdatePsu --file <filename> --address <PSU slave address> [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdatePsu --
file Supermicro_PSU.x0 --address 0x80
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdatePsu --
file Supermicro_PSU.x0 --index 1 --reboot --post_complete
```

```
Managed system..........192.168.34.56
    PSU index...........1
    PSU model...........PWS-5K26G-2R
    PSU FW revision......1.0.0
    PSU HW revision......1.2


Local PSU image file.....Supermicro_PSU.x0
    PSU model...........PWS-5K26G-2R
    PSU FW revision......1.0.1
    PSU HW revision......1.2

Status: Start updating PSU for 192.168.34.56

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


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

Preparing updating PSU...Done
```

```
Updating FW...>>>
```

```
Preparing updating PSU...Done

Updating FW...>>>
```

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.

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c UpdatePsu --file
Supermicro_PSU.x0 --address 0x80
```

```
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
```

5.9.3. 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 [--json_view]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetPowerStatus [--json_view]
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 GetPowerStatus [--json_view] [--remote_saa <remote SAA path>]
Multiple System	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetPowerStatus [--json_view]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c GetPowerStatus [--json_view] [--remote_saa <remote SAA path>]

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
    PSU consumption..........N/A
    Power Consumption
          Last Hour
              Average Usage...158.083333 (W)
              Max Peak........228 (W)
              Max Peak Time...2024-11-07T01:37:16+00:00
              Min Peak........123 (W)
              Min Peak Time...2024-11-07T01:52:16+00:00
          Last Day
              Average Usage...155.666667 (W)
              Max Peak........241 (W)
              Max Peak Time...2024-11-06T08:57:16+00:00
              Min Peak........64 (W)
              Min Peak Time...2024-11-06T07:57:16+00:00
          Last Week
              Average Usage...105.571429 (W)
              Max Peak........241 (W)
              Max Peak Time...2024-11-07T01:57:16+00:00
              Min Peak........0 (W)
              Min Peak Time...2024-11-01T13:57:16+00:00
```

The console output contains the following information for the GB200 system.

```
Managed system.............192.168.34.56
    System
        Power status.........PoweringOn
    Baseboard
        Power status.........Off
    Power Consumption
        Total GPU............842.609 (W)
        CPU 1................89.287000 (W)
        CPU 2................94.559000 (W)
        GPU 1................204.876000 (W)
        GPU 2................228.234000 (W)
        GPU 3................212.608000 (W)
        GPU 4................196.884000 (W)
```

In-Band:

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

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GetPowerStatus --remote_saa /root/saa
```

The console output contains the following information.

```
Managed system.................localhost
    Power status..............On
    PSU consumption...........N/A
```

In-Band Redfish Host Interface:

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

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 GetPowerStatus --remote_saa /root/saa
```

The console output contains the following information.

```
Managed system.................169.254.3.254
    Power status..............On
    Power Consumption
          Last Hour
              Average Usage...159.416667 (W)
              Max Peak........241 (W)
              Max Peak Time...2024-11-07T02:05:11+00:00
              Min Peak........123 (W)
              Min Peak Time...2024-11-07T01:50:11+00:00
          Last Day
              Average Usage...155.666667 (W)
              Max Peak........241 (W)
              Max Peak Time...2024-11-06T09:10:11+00:00
              Min Peak........64 (W)
              Min Peak Time...2024-11-06T08:10:11+00:00
          Last Week
              Average Usage...105.571429 (W)
              Max Peak........241 (W)
              Max Peak Time...2024-11-07T02:10:11+00:00
              Min Peak........0 (W)
              Min Peak Time...2024-11-01T14:10:11+00:00
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetPowerStatus
```

```
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 GetPowerStatus
```

```
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 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 7 = nmi 8 = on

Note: `up` maps to Redfish `ForceOn`, and `on` maps to Redfish `On`. The supported `--action` values listed below are extracted from the Redfish `ResetActionInfo` response.

- For **GB200 systems**, use the following command to fetch supported actions:

```
curl -k -X GET \
  -H "Content-Type: application/json" \
  -u "ADMIN:ADMIN" \
  "https://<BMC_IP>/redfish/v1/Systems/System_0/ResetActionInfo"
```

Response:


```
{
  "@odata.id": "/redfish/v1/Systems/System_0/ResetActionInfo",
  "@odata.type": "#ActionInfo.v1_1_2.ActionInfo",
  "Id": "ResetActionInfo",
  "Name": "Reset Action Info",
  "Parameters": [
    {
      "AllowableValues": [
        "ForceOff",
        "PowerCycle",
        "Nmi",
        "GracefulShutdown",
        "On",
        "ForceOn",
        "GracefulRestart",
        "ForceRestart"
      ],
      "DataType": "String",
```

```
      "Name": "ResetType",
      "Required": true
    }
  ]
}
```

- For **Supermicro BMC systems**, use this endpoint:

```
curl -k -X GET \
  -H "Content-Type: application/json" \
  -u "ADMIN:ADMIN" \
  "https://<BMC_IP>/redfish/v1/Systems/1/ResetActionInfo"
```

Response:

```
{
  "@odata.type": "#ActionInfo.v1_4_2.ActionInfo",
  "@odata.id": "/redfish/v1/Systems/1/ResetActionInfo",
  "Id": "ResetActionInfo",
  "Name": "Reset Action Info",
  "Parameters": [
    {
      "Name": "ResetType",
      "Required": true,
      "DataType": "String",
      "AllowableValues": [
        "On",
        "ForceOff",
        "GracefulShutdown",
        "GracefulRestart",
        "ForceRestart",
        "Nmi",
        "ForceOn",
        "PowerCycle"
      ]
    }
  ],
  "Oem": {},
  "@odata.etag": "\"46e93867384bf42fd07406c413b9b393\""
}
```

Syntax of SetPowerAction:

Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c SetPowerAction --action <action> [--interval <time interval>] [--power_on] [--post_complete]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c SetPowerAction --action <action> [--interval <time interval>]
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 SetPowerAction --action <action> [--interval <time interval>] [--remote_saa <remote SAA path>]
Multiple System	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SetPowerAction --action <action> [--interval <time interval>] [--power_on] [--post_complete]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c SetPowerAction --action <action> [--interval <time interval>] [--remote_saa <remote SAA path>]

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
```

In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -c SetPowerAction --action up
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c SetPowerAction --action up --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 SetPowerAction --action up --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetPowerAction --action up
```

```
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 SetPowerAction --action up
```

```
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 BIOS and BMC capabilities of the managed system will be shown in the “Execution Message” section in the created log file.



Notes:

- The supported power cycle interval depends on each managed system; the common range is between 5 and 255.
- When using the --post_complete option, the --power_on option is required. Note that the --power_on option only works with the AcCycle action and cannot be used for in-band usage.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> [--remote_saa &<remote SAA path>] -c GetAcpiPowerStatus
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetAcpiPowerStatus
Remote In-Band	saa -I Remote_INB -l <system list file> [--remote_saa <remote SAA path>] -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 GetLimitPolicyId = Gets limiting policy ID GetPsysInfo = Gets Psys information

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 [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action EnableGlobal [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action EnableGlobal [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action EnableGlobal [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action EnableGlobal [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type NM20 --action EnableGlobal --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action EnableGlobal --remote_saa /root/saa
```

```
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.

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 [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action DisableGlobal [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action DisableGlobal [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action DisableGlobal [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action DisableGlobal [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action DisableGlobal --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 -
-action DisableGlobal --remote_saa /root/saa
```

```
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.

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

--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 EnableDomain --domain_id <domain ID> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action EnableDomain --domain_id <domain ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action EnableDomain --domain_id <domain ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action EnableDomain --domain_id <domain ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action EnableDomain --domain_id <domain ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action EnableDomain --domain_id 0 --
remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 -
-action EnableDomain --domain_id 0 --remote_saa /root/saa
```

```
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.

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> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action DisableDomain --domain_id <domain ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action DisableDomain --domain_id <domain ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action DisableDomain --domain_id <domain ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action DisableDomain --domain_id <domain ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type NM20 --action DisableDomain --domain_id 0 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action DisableDomain --domain_id 0 --remote_saa /root/saa
```

```
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.

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> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type NM20 --action EnablePolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 -
-action EnablePolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

```
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.

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
--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 DisablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type NM20 --action DisablePolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action DisablePolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

```
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.

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	For the AddPowerPolicy action: Sets the aggressive CPU power correction mode to automatic mode by default. For the AddPolicy action: Specifies aggressive CPU power correction mode. 0: Automatic mode 1: Force non-aggressive mode 2: Force aggressive mode
--period	Specifies statistics reporting period in seconds.
--exception_action	For the AddPowerPolicy action: Specifies the policy exception action that sends the alert by default. For the AddPolicy 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	For the AddPowerPolicy action: 0: Entire platform 1: CPU subsystem

	2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem If the --domain option is not provided, sets the domain ID to Entire platform by default. For the AddPolicy action: 0: Entire platform 1: CPU subsystem 2: Memory subsystem 3: HW Protection 4: High Power I/O subsystem
--trigger_type	For the AddPowerPolicy action: Specifies the policy trigger type to no policy trigger by default. For the AddPolicy action: 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: MGPIO policy trigger
--trigger_limit	For the AddPowerPolicy action: Specifies the policy trigger limit to be the same as the policy target limit by default. For AddPolicy action: Specifies policy trigger limit.
--overwrite	Overwrite the policy.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action AddPowerPolicy [--domain_id <domain ID>] --policy_id <policy ID> --limit <limit> --time <time> --period <period> [--overwrite] [--json_view] saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> [--overwrite] [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action AddPowerPolicy [--domain_id <domain ID>] --policy_id <policy ID> --limit <limit> --time <time> --period <period> [--overwrite] [--json_view]

	saa -c PowerPolicy --type NM20 --action AddPolicy --type NM20 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> [--overwrite] [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action AddPowerPolicy [--domain_id <domain ID>] --policy_id <policy ID> --limit <limit> --time <time> --period <period> [--overwrite] [--remote_saa <remote SAA path>] [--json_view] saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action AddPolicy --type NM20 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> [--overwrite] [--remote_saa <remote SAA path>] [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action AddPowerPolicy [--domain_id <domain ID>] --policy_id <policy ID> --limit <limit> --time <time> --period <period> [--overwrite] [--json_view] saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> [--overwrite] [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action AddPowerPolicy [--domain_id <domain ID>] --policy_id <policy ID> --limit <limit> --time <time> --period <period> [--overwrite] [--remote_saa <remote SAA path>] [--json_view] saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> [--overwrite] [--remote_saa <remote SAA path>] [--json_view]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action AddPowerPolicy --policy_id 1 --limit
200 --time 20000 --period 200 --overwrite --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-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 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action AddPowerPolicy --policy_id 1 --limit 200 --time 20000 --period 200 --overwrite --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -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 --remote_saa /root/saa
```

```
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.

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> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type NM20 --action GetPolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action GetPolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

```
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.

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> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type NM20 --action DelPolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action DelPolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

```
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.

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 [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action ScanPolicy [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action ScanPolicy [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action ScanPolicy [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action ScanPolicy [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action ScanPolicy --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action ScanPolicy --remote_saa /root/saa
```

```
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.

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
--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 GetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action GetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action

	GetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action GetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action GetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type NM20 --action GetAlertThreshold --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action GetAlertThreshold --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

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

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> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action SetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> --count <count> --value <value> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action SetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> --count <count> --value <value> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action SetAlertThreshold --domain_id <domain ID> --policy_id <policy ID> --count <count> --value <value> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action SetAlertThreshold --domain_id 0 --
policy_id 1 --count 3 --value 100,200,300 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 -
-action SetAlertThreshold --domain_id 0 --policy_id 1 --count 3 --value
100,200,300 --remote_saa /root/saa
```

```
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.

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> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action GetPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action GetPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action GetPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action GetPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action GetPeriod --domain_id 0 --policy_id 0
--remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 -
-action GetPeriod --domain_id 0 --policy_id 0 --remote_saa /root/saa
```

```
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.

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> [--json_view]
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> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action AddPeriod --domain_id <domain ID> --policy_id <policy ID> --st <start time> --et <end time> --days <Days> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action AddPeriod --domain_id <domain ID> --policy_id <policy ID> --st

	<start time> --et <end time> --days <Days> [--json_view] [--remote_saa <remote SAA path>]

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
==========================================
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type NM20 --action AddPeriod --domain_id 0 --policy_id 0 --st 0000 --et 0006 --days 123 --remote_saa /root/saa
```

Multiple OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 --action AddPeriod --domain_id 0 --policy_id 0 --st 0000 --et 0006 --days 123 --remote_saa /root/saa
```

```
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.

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
--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
--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> [--json_view]
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> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS 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> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -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> [--json_view] [--remote_saa <remote SAA path>]

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
==========================================
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action UpdatePeriod --domain_id 0 --
policy_id 0 --period_id 1 --st 0000 --et 0006 --days 123 --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 -
-action UpdatePeriod --domain_id 0 --policy_id 0 --period_id 1 --st 0000
--et 0006 --days 123 --remote_saa /root/saa
```

```
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.

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
--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
--period_id	Period ID 1~5 for which policy should be used

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type NM20 --action DeletePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action DeletePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action DeletePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action DeletePeriod --domain_id <domain ID> --policy_id <policy ID> --period_id <Period ID> [--json_view] [--remote_saa <remote SAA path>]

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
==========================================
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action DeletePeriod --domain_id 0 --
policy_id 0 --period_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type NM20 -
-action DeletePeriod --domain_id 0 --policy_id 0 --period_id 1 --
remote_saa /root/saa
```

```
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.

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
--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 ClearPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view]
In-Band	saa -c PowerPolicy --type NM20 --action ClearPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type NM20 --action ClearPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type NM20 --action ClearPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type NM20 --action ClearPeriod --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type NM20 --action ClearPeriod --
domain_id 0 --policy_id 0
```

The console output contains the following information.

```
Done
==========================================
Domain ID = 0 , Policy ID = 0
==========================================
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type NM20 --action ClearPeriod --domain_id 0 --policy_id
0 --remote_saa /root/saa
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
NM20 --action ClearPeriod --domain_id 0 --policy_id 0
```

```
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 PowerPolicy --type NM20 -
-action ClearPeriod --domain_id 0 --policy_id 0 --remote_saa /root/saa
```

```
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.

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 Platform Power (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 [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action EnableGlobal [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action EnableGlobal [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action EnableGlobal [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action EnableGlobal [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type BMC10 --action EnableGlobal --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action EnableGlobal --remote_saa /root/saa
```

```
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 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.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action DisableGlobal [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action DisableGlobal [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action DisableGlobal

	[--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action DisableGlobal [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action DisableGlobal [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type BMC10 --action DisableGlobal --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10 --action DisableGlobal --remote_saa /root/saa
```

```
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 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> [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action EnableDomain --domain_id <domain ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action EnableDomain --domain_id <domain ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action EnableDomain --domain_id <domain ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action EnableDomain --domain_id <domain ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type BMC10 --action EnableDomain --domain_id 0 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10 --action EnableDomain --domain_id 0 --remote_saa /root/saa
```

```
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 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> [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action DisableDomain --domain_id <domain ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action DisableDomain --domain_id <domain ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action DisableDomain --domain_id <domain ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action DisableDomain --domain_id <domain ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type BMC10 --action DisableDomain --domain_id 0 --
remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action DisableDomain --domain_id 0 --remote_saa /root/saa
```

```
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 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> [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action EnablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type BMC10 --action EnablePolicy --domain_id 0 --
policy_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action EnablePolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

```
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 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> [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type BMC10 --action DisablePolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action DisablePolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

```
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 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	Limits the target to reach the corresponding power level when the trigger limit is reached. For AddPowerPolicy action: Specifies policy target limit (watts) from 0 to 32767. 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.

--mode	For the AddPowerPolicy action: Sets the aggressive CPU power correction mode to automatic mode by default. For the AddPolicy action: Specifies aggressive CPU power tuning mode. 0: Automatic mode 1: Force non-aggressive mode 2: Force aggressive mode If the --mode option is not provided, the default mode is Automatic mode.
--period	Specifies statistics reporting period in seconds from 1 to 3600.
--exception_action	For the AddPowerPolicy action: Specifies the policy exception action that sends the alert by default. For the AddPolicy action: Specifies the policy exception action. 1: Sends alert 2: Shutdowns system 3: Sends alert and shutdowns system
--time	Specifies the correction time limit (ms) from 1000 to 60000 for the use of the exception action.
--policy_id	Specifies 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)
--trigger_type	For the AddPowerPolicy action: Specifies the policy trigger type to no policy trigger by default. For the AddPolicy action: Specifies the 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 6: MGPIO policy trigger 7: C0 Residency in [%] 8: Host Reset 9: SMBAlert Interrupt
--trigger_limit	For the AddPowerPolicy action: Specifies the policy trigger limit to be the same as the policy target limit by default.

	For AddPolicy action: 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. 0: Persistent storage 1: Volatile memory
--overwrite	Overwrites the policy.



Note: The --period (Statistic Reporting Period) option is used to specify the period for calculating average power when BMC Intel Node Manager reports power Manager reports performance statistics.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action AddPowerPolicy --domain_id <domain ID> --policy_id <policy ID> --limit <limit> --time <time> --period <period> --storage <storage> [--overwrite] [--json_view] saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> --storage <storage> [--overwrite] [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action AddPowerPolicy --domain_id <domain ID> --policy_id <policy ID> --limit <limit> --time <time> --period <period> --storage <storage> [--overwrite] [--json_view] saa -c PowerPolicy --type BMC10 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> --storage <storage> [--overwrite] [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action AddPowerPolicy --domain_id <domain ID> --policy_id <policy ID> --

	limit <limit> --time <time> --period <period> --storage <storage> [--overwrite] [--json_view] [--remote_saa <remote SAA path>] saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> --storage <storage> [--overwrite] [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action AddPowerPolicy --domain_id <domain ID> --policy_id <policy ID> --limit <limit> --time <time> --period <period> --storage <storage> [--overwrite] [--json_view] saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> --storage <storage> [--overwrite] [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action AddPowerPolicy --domain_id <domain ID> --policy_id <policy ID> --limit <limit> --time <time> --period <period> --storage <storage> [--overwrite] [--json_view] [--remote_saa <remote SAA path>] saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action AddPolicy --domain_id <domain ID> --policy_id <policy ID> --trigger_type <trigger type> --mode <mode> --exception_action <exception action> --limit <limit> --time <time> --trigger_limit <trigger limit> --period <period> --storage <storage> [--overwrite] [--json_view] [--remote_saa <remote SAA path>]

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

Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type BMC10 --action AddPowerPolicy --domain_id 0 --policy_id 1 --limit 200 --time 20000 --period 200 --storage 1 --overwrite --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -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 --remote_saa /root/saa

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action AddPowerPolicy --domain_id 0 --policy_id 1 --limit 200 --time
20000 --period 200 --storage 1 --overwrite --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -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 --remote_saa /root/saa
```

```
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.

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
--policy_id	Specifies 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 GetPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]

In-Band	saa -c PowerPolicy --type BMC10 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action GetPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type BMC10 --action GetPolicy --domain_id 1 --policy_id
60 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action GetPolicy --domain_id 1 --policy_id 60 --remote_saa /root/saa
```

```
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.

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

--policy_id	Specifies 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 DelPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action DelPolicy --domain_id <domain ID> --policy_id <policy ID> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type BMC10 --action DelPolicy --domain_id 0 --policy_id
1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action DelPolicy --domain_id 0 --policy_id 1 --remote_saa /root/saa
```

```
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.

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 [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action ScanPolicy [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action ScanPolicy [--

	json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action ScanPolicy [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action ScanPolicy [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type BMC10 --action ScanPolicy --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action ScanPolicy --remote_saa /root/saa
```

```
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.

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 [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action GetLimitPolicyId [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action GetLimitPolicyId [--json_view] [--remote_saa <remote SAA path>]

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action GetLimitPolicyId [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action GetLimitPolicyId [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c PowerPolicy --type BMC10 --action GetLimitPolicyId --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c PowerPolicy --type BMC10
--action GetLimitPolicyId --remote_saa /root/saa
```

```
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.

5.9.6.2.12. Getting Platform Power Information

Use the PowerPolicy command with the --action GetPsysInfo option to get Platform Power (Psys) information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c PowerPolicy --type BMC10 --action GetPsysInfo [--json_view]
In-Band	saa -c PowerPolicy --type BMC10 --action GetPsysInfo [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c PowerPolicy --type BMC10 --action GetPsysInfo [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c PowerPolicy --type BMC10 --action GetPsysInfo [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c PowerPolicy --type BMC10 --action GetPsysInfo [--json_view] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c PowerPolicy --
type BMC10 --action GetPsysInfo
```

The console output contains the following information.

```
Psys support.............Yes
```

In-Band:

```
[SAA_HOME]# ./saa -c PowerPolicy --type BMC10 --action GetPsysInfo
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c PowerPolicy --type BMC10 --action GetPsysInfo --remote_saa /root/saa
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c PowerPolicy --type
BMC10 --action GetPsysInfo
```

```
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 PowerPolicy --type BMC10
--action GetPsysInfo --remote_saa /root/saa
```

```
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.

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 GetAssetTag = Get asset tag string SetAssetTag = Set asset tag 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 Intel's 14th generation platforms, only the following --action values with --type STD_DCMI are supported: SetMCID, GetMCID, GetPowerStatus, SetAssetTag, and GetAssetTag. All other actions under STD_DCMI type and any actions under NM20 type are not supported by bMC on these platforms.

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>] [--json_view]
Remote In-Band	saa -I Remote_INB -u <username> -p <password>} --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type STD_DCMI --action Find [--start_ip <start IP> --end_ip <end IP> --netmask <netmask>] [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type STD_DCMI --action Find [--start_ip <start IP> --end_ip <end IP> --netmask <netmask>] [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DcmiManage --type STD_DCMI --action Find --start_ip 192.168.34.1 --
end_ip 192.168.34.100 --netmask 255.255.255.0

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DcmiManage --type STD_DCMI --action Find --start_ip 192.168.34.1 --
```

```
end_ip 192.168.34.100 --netmask 255.255.255.0 --json_view
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type
STD_DCMI --action Find --start_ip 192.168.34.1 --end_ip 192.168.34.100 --
netmask 255.255.255.0
```

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type
STD_DCMI --action Find --start_ip 192.168.34.1 --end_ip 192.168.34.100 --
netmask 255.255.255.0 --json_view
```

```
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 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.

5.9.7.1.2. 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 [--json_view]
In-Band	saa -c DcmiManage --type STD_DCMI --action GetCap [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type STD_DCMI --action GetCap [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action GetCap [--json_view]

Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type STD_DCMI --action GetCap [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DcmiManage --type STD_DCMI --action GetCap
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type
STD_DCMI --action GetCap
```

```
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.

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 [--json_view]
In-Band	saa -c DcmiManage --type STD_DCMI --action GetPowerStatus [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type STD_DCMI --action GetPowerStatus [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action GetPowerStatus [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type STD_DCMI --action GetPowerStatus [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DcmiManage --type STD_DCMI --action GetPowerStatus
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type
STD_DCMI --action GetPowerStatus
```

```
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.

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 [--json_view]
In-Band	saa -c DcmiManage --type STD_DCMI --action GetMCID [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type STD_DCMI --action GetMCID

	[--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action GetMCID [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type STD_DCMI --action GetMCID [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type STD_DCMI --action GetMCID
```

```
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.

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> [--json_view]
In-Band	saa -c DcmiManage --type STD_DCMI --action SetMCID --value <value> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type STD_DCMI --action SetMCID --value <value> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action SetMCID --value <value> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type STD_DCMI --action SetMCID --value <value> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type
STD_DCMI --action SetMCID --value example
```

```
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.

5.9.7.1.6. Getting Asset Tag String

Use the DcmiManage command with the --action GetAssetTag option to get the asset tag value from a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type STD_DCMI --action GetAssetTag [--json_view]
In-Band	saa -c DcmiManage --type STD_DCMI --action GetAssetTag [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type STD_DCMI --action GetAssetTag [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action GetAssetTag [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type STD_DCMI --action GetAssetTag [--json_view] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type STD_DCMI --action GetAssetTag
```

In-Band:

```
[SAA_HOME]# ./saa -c DcmiManage --type STD_DCMI --action GetAssetTag
```

The console output contains the following information.

```
Asset Tag: AssetTag_example
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c DcmiManage --type STD_DCMI --action GetAssetTag
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type
STD_DCMI --action GetAssetTag
```

```
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 DcmiManage --type
STD_DCMI --action GetCap
```

```
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.

5.9.7.1.7. Setting Asset Tag String

Use the DcmiManage command with the --action option SetAssetTag to set the asset tag string from a managed system.
The following is the supported option for the --action SetAssetTag option.

Option	Description
--value	Asset tag string value.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c DcmiManage --type STD_DCMI --action SetAssetTag --value <value> [--json_view]
In-Band	saa -c DcmiManage --type STD_DCMI --action SetAssetTag --value <value> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type STD_DCMI --action

	SetAssetTag --value <value> [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type STD_DCMI --action SetAssetTag --value <value> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type STD_DCMI --action SetAssetTag --value <value> [--json_view] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c DcmiManage --type STD_DCMI --action SetAssetTag --value example
```

In-Band:

```
[SAA_HOME]# ./saa -c DcmiManage --type STD_DCMI --action SetAssetTag --value example
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c DcmiManage --type STD_DCMI --action SetAssetTag --value example
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c DcmiManage --type STD_DCMI --action SetAssetTag --value example
```

```
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 DcmiManage --type STD_DCMI --action SetAssetTag --value example
```

```
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.

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 [--json_view]
In-Band	saa -c DcmiManage --type NM20 --action GetCap [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type NM20 --action GetCap [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l< system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action GetCap [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type NM20 --action GetCap [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DcmiManage --type NM20 --action GetCap
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type NM20 --
action GetCap
```

```
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.

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>] [--json_view]
In-Band	saa -c DcmiManage --type NM20 --action GetPowerReading --mode <mode> [--period <period>] [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type NM20 --action GetPowerReading --mode <mode> [--period <period>] [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action GetPowerReading --mode <mode> [--period <period>] [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type NM20 --action GetPowerReading --mode <mode> [--period <period>] [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c DcmiManage --type NM20 --action GetPowerReading --mode 2 --period 05
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type NM20 --action GetPowerReading --mode 2 –-period 05
```

```
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.

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 [--json_view]
In-Band	saa -c DcmiManage --type NM20 --action GetPowerLimit [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type NM20 --action GetPowerLimit [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action GetPowerLimit [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type NM20 --action GetPowerLimit [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DcmiManage --type NM20 --action GetPowerLimit
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type NM20 --
action GetPowerLimit
```

```
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.

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> [--json_view]
In-Band	saa -c DcmiManage --type NM20 --action SetPowerLimit --exception_action <exception action> --limit <limit> --time <time> --period <period> [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type NM20 --action SetPowerLimit --exception_action <exception action> --limit <limit> --time <time> --period <period> [--json_view] [--remote_saa <remote SAA path>]
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> [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type NM20 --action SetPowerLimit --exception_action <exception action> --limit <limit> --time <time> --period <period> [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c DcmiManage --type NM20 --action SetPowerLimit --exception_action 1 --
limit 200 --time 20000 --period 50
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type NM20 --
action SetPowerLimit --exception_action 1 --limit 200 --time 20000 --
period 50
```

```
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.

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 [--json_view]
In-Band	saa -c DcmiManage --type NM20 --action EnablePowerLimit [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type NM20 --action EnablePowerLimit [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action EnablePowerLimit [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type NM20 --action EnablePowerLimit [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type NM20 --
action EnablePowerLimit
```

```
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.

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 [--json_view]
In-Band	saa -c DcmiManage --type NM20 --action DisablePowerLimit [--json_view]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c DcmiManage --type NM20 --action DisablePowerLimit [--json_view] [--remote_saa <remote SAA path>]

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c DcmiManage --type NM20 --action DisablePowerLimit [--json_view]
Remote In-Band	saa -I Remote_INB -l <system list file> -c DcmiManage --type NM20 --action DisablePowerLimit [--json_view] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c DcmiManage --type NM20 --action DisablePowerLimit
```

```
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.

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 -I 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."

Single System	
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>
Multiple Systems	
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.

5.9.11. Getting and Setting CPU Power Limit of the managed system

Command Options	Descriptions
--action	Sets action to: 1 = GetPowerLimit 2 = SetPowerLimitEnabled 3 = SetPowerLimitDisabled

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c CpuPowerManage --action <action> --value <value>
In-Band	saa -c CpuPowerManage --action <action> --value <value>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c CpuPowerManage --action <action> --value <value>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c CpuPowerManage --action <action> --value <value>
Remote In-Band	saa -I Remote_INB -l <system list file> -c CpuPowerManage --action <action> --value <value>

Example:

OOB:

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

The console output contains the following information for ARM system.

```
[ARM System]
    The CPU SoC power limit is 220 Watts.
```

The console output contains the following information for AMD system.

```
[AMD System]
    The CPU Package Power Consumption is 42304 mWatts.
    The CPU SoC power limit is 240000 mWatts.
    The CPU SoC Max power limit is 240000 mWatts.
    The CPU current cTDP is 240000 mWatts.
    The CPU Max cTDP is 240000 mWatts.
    The CPU Min cTDP is 225000 mWatts.
```

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CpuPowerManage --action SetPowerLimitEnabled --value 400

The console output contains the following information.

```
.............................
The Cpu SoC power limit setting successfully.
```

In-Band:

[SAA_HOME]# ./saa -c CpuPowerManage --action SetPowerLimitEnabled

[SAA_HOME]# ./saa -c CpuPowerManage --action SetPowerLimitEnabled --value 400

Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c CpuPowerManage --action GetPowerLimit --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c CpuPowerManage --action SetPowerLimitEnabled --value 700 --remote_saa /root/saa

Multiple Systems OOB:

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p ADMIN -c CpuPowerManage --action GetPowerLimit

```
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 CpuPowerManage --action
GetPowerLimit --remote_saa /root/saa
```

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

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.

5.9.12. Getting PowerShelf Information

Use the “GetPowerShelfInfo” command to get the current PowerShelf information and power units information from the managed system. According to the PMC web UI, "GetPowerShelfInfo" displays the same information in the console.

Single System	
OOB	saa -i <BMC IP> -u <username> -p <password> -c GetPowerShelfInfo [--dev_id <ID>] [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetPowerShelfInfo [--dev_id <ID>] [--json_view]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.59 -u ADMIN -p PASSWORD -c
GetPowerShelfInfo
```

Console output.

```
[PowerShelf]
    State.................. Standby
```

```
    Power................. On
    Health Rollup......... OK
    Number of Input Source 1
    Name.................. chassis
    Part Number........... PF-1333-7R
    Serial Number......... 613337RXX03X3429064
    Model Name............ PF-1333-7R
    Hardware Version...... X3
    Power Rating.......... 33000
    Manufacturer.......... LITE-ON TECHNOLOGY CORP.
    Chassis Type.......... Power Shelf

[Power Unit 0]
    Status................ OK
    State................. Standby
    Input Voltage......... 242.0 V
    Input Current......... 2.50 A
    Input Power........... 598.0 W
    Output Voltage........ 49.70 V
    Output Current........ 11.10 A
    Output Power.......... 590.0 W
    Ambient Temp.......... 55.0 °C
    Fan................... 6080.0 RPMS
    Serial Number......... 6PL1R01X34282AC
    Firmware Version...... 0x6 / 0x8
    Model Name............ SP-2552-1R

[Power Unit 1]
    Status................ OK
    State................. Standby
    Input Voltage......... 242.0 V
    Input Current......... 2.50 A
    Input Power........... 592.0 W
    Output Voltage........ 49.91 V
    Output Current........ 11.23 A
    Output Power.......... 568.0 W
    Ambient Temp.......... 56.75 °C
    Fan................... 6080.0 RPMS
    Serial Number......... 6PL1R01X342827W
    Firmware Version...... 0x6 / 0x8
    Model Name............ SP-2552-1R

[Power Unit 2]
    Status................ OK
    State................. Standby
    Input Voltage......... 240.25 V
    Input Current......... 2.67 A
    Input Power........... 622.0 W
    Output Voltage........ 49.83 V
    Output Current........ 11.43 A
    Output Power.......... 576.0 W
    Ambient Temp.......... 53.50 °C
    Fan................... 6016.0 RPMS
```

```
    Serial Number......... 6PL1R01X34282CP
    Firmware Version...... 0x6 / 0x8
    Model Name............ SP-2552-1R

[Power Unit 3]
    Status................ OK
    State................. Standby
    Input Voltage......... 242.50 V
    Input Current......... 2.43 A
    Input Power........... 576.0 W
    Output Voltage........ 49.87 V
    Output Current........ 11.07 A
    Output Power.......... 543.0 W
    Ambient Temp.......... 57.0 °C
    Fan................... 11776.0 RPMS
    Serial Number......... 6PL1R01X34282K7
    Firmware Version...... 0x6 / 0x8
    Model Name............ SP-2552-1R

[Power Unit 4]
    Status................ OK
    State................. Standby
    Input Voltage......... 244.0 V
    Input Current......... 2.06 A
    Input Power........... 477.0 W
    Output Voltage........ 49.60 V
    Output Current........ 9.75 A
    Output Power.......... 465.50 W
    Ambient Temp.......... 72.75 °C
    Fan................... 3712.0 RPMS
    Serial Number......... 6PL1R01X34282D4
    Firmware Version...... 0x3 / 0x3
    Model Name............ SP-2552-1R

[Power Unit 5]
    Status................ OK
    State................. Standby
    Input Voltage......... 240.0 V
    Input Current......... 2.18 A
    Input Power........... 520.0 W
    Output Voltage........ 49.72 V
    Output Current........ 9.75 A
    Output Power.......... 470.0 W
    Ambient Temp.......... 74.75 °C
    Fan................... 3648.0 RPMS
    Serial Number......... 6PL1R01X34282KE
    Firmware Version...... 0x3 / 0x3
    Model Name............ SP-2552-1R
```

```
[SAA_HOME]# ./saa -i 192.168.34.59 -u ADMIN -p PASSWORD -c
GetPowerShelfInfo --dev_id 0
```

```
[PowerShelf]
    State.................. Standby
    Power.................. On
    Health Rollup......... OK
    Number of Input Source 1
    Name................... chassis
    Part Number........... PF-1333-7R
    Serial Number......... 613337RXX03X3429064
    Model Name............ PF-1333-7R
    Hardware Version...... X3
    Power Rating.......... 33000
    Manufacturer.......... LITE-ON TECHNOLOGY CORP.
    Chassis Type.......... Power Shelf

[Power Unit 0]
    Status................. OK
    State.................. Standby
    Input Voltage......... 242.0 V
    Input Current......... 2.50 A
    Input Power........... 598.0 W
    Output Voltage........ 49.70 V
    Output Current........ 11.10 A
    Output Power.......... 590.0 W
    Ambient Temp.......... 55.0 °C
    Fan.................... 6080.0 RPMS
    Serial Number......... 6PL1R01X34282AC
    Firmware Version...... 0x6 / 0x8
    Model Name............ SP-2552-1R
```

```
[SAA_HOME]# $ ./saa -c GetPowerShelfInfo -i 10.168.34.59 -p ADMIN -u ADMIN --json_view
```



Note: The “--json_view” option is used to show the PowerShelf and power units information in JSON format.

Multiple Systems OOB:

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

```
SList.txt:
    192.168.34.59
    192.168.34.60
```

If the execution “Status” field of the managed PowerShelf shows SUCCESS, the console output of the managed PowerShelf will be shown in the “Execution Message” section in the created log file.



Note:
This command is only available on the LiteOn PowerShelf System with CM-14MP-1R Power Management Controller.

5.9.13. Updating Power Unit Firmware in the PowerShelf

Use the “UpdatePowerShelf” command to update the power units firmware from the managed PowerShelf system.

Single System	
OOB	saa -i <BMC IP> -u <username> -p <password> -c UpdatePowerShelf --file <file name with path> --dev_id <ID>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdatePowerShelf --file <file name with path> --dev_id <ID>

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.59 -u ADMIN -p PASSWORD -c
UpdatePowerShelf --file ./SP-2552-
1R_0608_Bootloader_X3_X4_20250326.D2DAppA.tar --dev_id 1
```

```
    Managed system.................172.25.230.240
    Model..........................SP-2552-1R
    Name...........................power unit 1
    Current firmware version......0xf6 / 0x8
    Local firmware file...........SP-2552-
1R_0608_Bootloader_X3_X4_20250326.D2DAppA.tar

Status: start updating power unit 1 for 172.25.230.240

The firmware update request for power unit 1 was sent successfully.
```

```
The update procedure takes about 7 minutes.
Warning: Do not update other power unit devices until this update is completed.
.................................................
.................................................
.................................................
.................................................
.................................................
.................................................
.....................Done

Status: power unit 1 was successfully updated for 172.25.230.240
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdatePowerShelf --file ./SP-2552-1R_0608_Bootloader_X3_X4_20250326.D2DAppA.tar --dev_id 0
```

```
SList.txt:
    192.168.34.59
    192.168.34.60
```

If the execution “Status” field of the managed PowerShelf shows SUCCESS, the console output of the managed PowerShelf will be shown in the “Execution Message” section in the created log file.



Note:
This command is only available on the LiteOn PowerShelf System with CM-14MP-1R Power Management Controller.

5.10. PCIe-Switch Management

5.10.1. Getting PCIeSwitch Information

Use the “GetPCIeSwitchInfo” 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 GetPCIeSwitchInfo
In-Band	saa -c GetPCIeSwitchInfo [--file <filename> [--file_only]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetPCIeSwitchInfo

Example:

In-Band:

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

[SAA_HOME]# ./saa -c GetPCIeSwitchInfo --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 “UpdatePCIeSwitch” 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 UpdatePCIeSwitch {--dev_id <index>} {--file <filename>}
In-Band	saa -c UpdatePCIeSwitch {--dev_id <index>} {--file <filename>}

Example:

In-Band:

```
[SAA_HOME]# ./saa -c UpdatePCIeSwitch --file fw_file.img --dev_id 0
```

OOB:

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

Image Type..........................Firmware Image
    Version.........................04.11.00.00
Image Type..........................Manufacturing
    Revision........................0:23:24:82
    Platform Name...................AOM-SXM5-IO
    Local Firmware File.............fw_411.fw
Update firmware progress Started ...
Updating................................ (100%)
Update firmware success.

Note: Please do power cycle to activate the updated image.
```

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
        Local PCIeSwitch image file.....AOM_SXM5_IO_4.13GCA_24.102.174.fw

Uploading FW..
Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done
```



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 Switchchipsets, 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.

5.11. 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c RawCommand --raw <raw command> [--

	remote_saa <remote SAA path>]
Multiple System	
OOB	saa -l <system list file> [-u <username> -p <password>] -c RawCommand --raw <raw command>
Remote In-Band	saa -l <system list file> -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c RawCommand --raw <raw command> [--remote_saa <remote SAA path>]

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'
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c RawCommand --raw '06 01'

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c RawCommand --raw '06 01'

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c RawCommand --raw '0x06
0x01'
```

```
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 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c RawCommand --ipmb <raw command> [--remote_saa <remote SAA path>]
Multiple System	
OOB	saa -l <system list file> [-u <username> -p <password>] -c

	RawCommand --ipmb <raw command>
Remote In-Band	saa -l <system list file> -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c RawCommand --ipmb <raw command> [--remote_saa <remote SAA path>]

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'
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c RawCommand --ipmb '06 01'

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c RawCommand --ipmb '0x06 0x01'
```

The console output contains the following information.

```
00
57 01 00 4C 00
```

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c RawCommand --ipmb '06 01'

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c RawCommand --ipmb '0x06
0x01'
```

```
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 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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetUsbAccessMode [--remote_saa <remote SAA path>]
Multiple Systems	
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetUsbAccessMode [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetUsbAccessMode
```

```
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 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.

5.11.4. 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}
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SetUsbAccessMode --panel <front|rear> {--disable | --enable} [--remote_saa <remote SAA path>]
Multiple Systems	
Remote In-Band	saa -I Remote_INB -l <system list file> -c SetUsbAccessMode --panel <front|rear> {--disable | --enable} [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c SetUsbAccessMode --panel rear --disable
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SetUsbAccessMode --panel
rear --enable
```

```
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 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:
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 modify the KMS server configurations, upload TLS certificates and test the connection to the KMS server.

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…]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> [--remote_saa <remote SAA path>] -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 [options…]
Remote In-Band	saa -I Remote_INB -l <system list file> [--remote_saa <remote SAA path>] -c KmsManage [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.
--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.

For Multiple Systems usage, the managed systems should be enumerated row by row in the system list file. For the “KmsManage” command, the system list file format is fixed for specific commands. Please refer to 5.4.3. Getting Current BIOS Settings.

Example:

OOB:

```
[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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-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 Remote_INB --oi 192.168.34.57 --ou root --op 111111
-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 Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c KmsManage --action DeleteAll --reboot

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c KmsManage --action GetInfo
```

The console output contains the following information.

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

    KMS Server IP..................192.168.12.78
    Second KMS Server IP...........192.168.12.79
    KMS TCP Port Number............5696
    KMS Time Out...................3
    KMS TimeZone...................GMT+0

    Client UserName................user123
    Client Password................******

    KMS TLS Certificate
    CA Certificate.................Uploaded
    Client Certifcate..............Uploaded
    Client Private Key.............Uploaded
    KMS Server Probe Status........KMS function works normally
```

Multiple Systems OOB:

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

```
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 KmsManage --action
GetInfo
```

```
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 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 option --item and option --value to configure the SOL parameter to a specific value.

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

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 --item non-volatile-bit-rate --value 115.2

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

The console output contains the following information.

```
Managed system.........................192.168.34.56
    Set in progress.....................set-complete
    Enabled.............................true
    Force Encryption....................false
    Force Authentication................false
    Privilege Level.....................OPERATOR
    Character Accumulate Level (ms).....0
    Character Send Threshold............0
    Retry Count.........................2
    Retry Interval (ms).................20
    Volatile Bit Rate (kbps)............115.2
    Non-Volatile Bit Rate (kbps)........115.2
    Payload Channel.....................1 (0x01)
    Payload Port........................623
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SOL --action Set --item retry-count --value 3

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c SOL --action Set --item force-encryption --value true
```

```
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 -I Redfish_HI -u <username> -p <password> -c RedfishApi --api <api path> [-v] [--request <http method>] [--file <file name> [--overwrite]] [--data <request body>] [--retry <number>]
Multiple Systems	
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	Desciption
--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>	The request body for the POST and PATCH methods. There are two usages: • Supplies the body in string directly. Note that the special character should be escaped. • Stores the body in a text file and supplies the file name. Note that you need to prepend an at character (@) to the file name, e.g., “--data @body.txt.”

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 separated 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 <promtp 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]]
Remote In-Band	saa -c GetUSBHostControllerInfo -l Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> [--remote_saa <remote SAA path>]
Multiple Systems	
Remote In-Band	saa -c GetUSBHostControllerInfo -l Remote_INB -l <system list file> [--remote_saa <remote SAA path>]

Example:

In-Band:

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

[SAA_HOME]# ./saa -c GetUSBHostControllerInfo --file fw_file_path --
file_only

[SAA_HOME]# ./saa -c GetUSBHostControllerInfo --cfg_file cfg_file_path --
file_only
```

The console output contains the following information for the Renesas µPD720201 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
```

The console output contains the following information for the ASMedia ASM3042 chipset on the X14SBH system.

```
Managed system.......................localhost
    Device ID(0)
        Bus............................0x3B
        Device.........................0x00
        Function.......................0x00
```

```
        FW Version.....................230802_71_02_40
        PCI Subsystem ID...............1d48
        PCI Subsystem Vendor ID.........15d9

    Firmware File.....................230802_71_1F_42.bin
        FW Version.....................230802_71_1f_42
        SubsyetemID....................N/A
        SubsyetemVendorID..............N/A
```

This command is available on the following platforms:

Platform	Chipset Information	Support OS
X14SBT-G	Renesas µPD720201	Ubuntu 20.04 and later Red Hat 9.0 and later
X14SBH	ASMedia ASM3042	Ubuntu 20.04 and later Red Hat 9.0 and later Windows Server



Notes:

- On the X14SBT-G platform with Renesas USB Host Controller µPD720201 chipset, execute the "make -f Makefile.drv" command in the “SAA/driver/renesas/USB” folder to build the device driver.
- 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 <fw_file_path>} [--cfg_file <cfg_file_path>] [--reboot]
Remote In-Band	saa -c UpdateUSBHostController -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> {--dev_id <index>} {--file <fw_file_path>} [--cfg_file <cfg_file_path>] [--reboot] [--remote_saa <remote SAA path>]

Multiple Systems	
Remote In-Band	saa -c UpdateUSBHostController -l Remote_INB -l <system list file> {--dev_id <index>} {--file <fw_file_path>} [--cfg_file <cfg_file_path>] [--reboot] [--remote_saa <remote SAA path>]

Example:

In-Band:

```
[SAA_HOME]# ./saa -c UpdateUSBHostController --dev_id 0 --file
fw_file_path [--cfg_file cfg_file_path]
```

The console output contains the following information for the Renesas µPD720201 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 successed.

Note: Please do power cycle to activate the updated image.
```

The console output contains the following information for the Renesas ASM3042 chipset on the X14SBH system.

```
Managed system.......................localhost
    Device ID(0)
```

```
        Bus.............................0x3B
        Device..........................0x00
        Function........................0x00
        FW Version......................230802_71_02_40
        PCI Subsystem ID................1d48
        PCI Subsystem Vendor ID.........15d9

    Firmware File.......................230802_71_1F_42.bin
        FW Version......................230802_71_1f_42
        SubsyetemID.....................N/A
        SubsyetemVendorID...............N/A


Start to update firmware.
Update firmware successed.

Note: Please do power cycle to activate the updated image.
```



Notes:

- Refer the available platforms table in Section 5.11.14 for the command supportable.
- On the X14SBT-G platform with Renesas USB Host Controller µPD720201 chipset, execute command "make -f Makefile.drv" in the “SAA/driver/renesas/USB” folder to build the device driver.
- 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> [--overwrite]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c RemoteScreenshot --file <filename.png> [--overwrite]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c

	RemoteScreenshot --file <filename.png> [--overwrite] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c RemoteScreenshot --file <filename.png> [--overwrite]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c RemoteScreenshot --file <filename.png> [--overwrite] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
RemoteScreenshot --file remotefile.png
```

In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c RemoteScreenshot
--file remotefile.png --overwrite
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.57 -
-ou root --op 111111 -c RemoteScreenshot --file remotefile.png --
overwrite
```

Multiple systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c RemoteScreenshot -
-file remotefile.png
```

```
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 RemoteScreenshot --file
remotefile.png
```

```
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 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.

5.11.17. 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.

5.11.18. Remote Screenvideo

This feature allows you to remotely record screen video on a target system. It's especially useful for debugging, as it can capture the screen during early boot stages — helping users review what was displayed right after the system powers on. The “RemoteScreenVideo” command supports the following features on systems:

- **Downloading Recorded Video**
  Use the “RemoteScreenVideo” command with the “--action Download” option to download the recorded video file. The video is saved in AVI format.

- **Enabling Screen Video Recording**
  Use the “RemoteScreenVideo” command with the “--action Enable” option to start recording the screen during system boot.

  The “--period” option must be used with this action to specify when the recording should stop:

  - “BufferFull”: Stops recording when the screen buffer is full.

- “POSTEnd”: Stops recording after the BIOS POST process completes.

- **Disabling Screen Video Recording**

  Use the “RemoteScreenVideo” command with the “--action Disable” option to stop the screen video recording configuration.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c RemoteScreenVideo --action <action> [--period <record period>] [--reboot [--post_complete]] [--file <filename.avi>] [--overwrite]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c RemoteScreenVideo --action <action> [--period <record period>] [--reboot] [--file <filename.avi>] [--overwrite]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c RemoteScreenVideo --action <action> [--period <record period>] [--reboot] [--file <filename.avi>] [--overwrite] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c RemoteScreenVideo --action <action> [--period <record period>] [--reboot [--post_complete]] [--file <filename.avi>] [--overwrite]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c RemoteScreenVideo --action <action> [--period <record period>] [--reboot] [--file <filename.avi>] [--overwrite] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
RemoteScreenVideo --action Enable --period POSTEnd --reboot --
post_complete

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
RemoteScreenVideo --action Download --file filename.avi --overwrite
```

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

In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c RemoteScreenVideo
--action Enable --period POSTEnd --reboot

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c RemoteScreenVideo
--action Download --file filename.avi --overwrite

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

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.33.12 -
-ou root --op 111111 -c RemoteScreenVideo --action Enable --period
POSTEnd --reboot --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.33.12 -
-ou root --op 111111 -c RemoteScreenVideo --action Download --file
filename.avi --overwrite --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.33.12 -
-ou root --op 111111 -c RemoteScreenVideo --action Disable --remote_saa
/root/saa
```

Multiple systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -c RemoteScreenVideo --action Enable --
period POSTEnd --reboot --post_complete

[SAA_HOME]# ./saa -l SList.txt -c RemoteScreenVideo --action Download --
file filename.avi --overwrite

[SAA_HOME]# ./saa -l SList.txt -c RemoteScreenVideo --action Disable
```

```
SList.txt (Multiple systems OOB):
    192.168.34.56 BMC_Username BMC_PASSWD
    192.168.34.57 BMC_Username BMC_PASSWD
```

Multiple systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c RemoteScreenVideo --
action Enable --period POSTEnd --reboot --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c RemoteScreenVideo --
action Download --file filename.avi --overwrite --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c RemoteScreenVideo --
action Disable --remote_saa /root/saa
```

```
SList.txt (Multiple systems Remote In-Band):
    192.168.34.56 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
    192.168.34.57 OS_Username OS_PASSWD BMC_Username BMC_PASSWD
```

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. 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 -l <system list file> [-u <username> -p <password>] -c GetGpuInfo [--showoam <oam id>] [--file <filename>]
Remote In-Band	saa -I Redish_HI -l <system list file> -c GetGpuInfo [--show_all] [--showoam <oam id>] [--file <filename>] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[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
            Configration ID.............01

        Device Id(1)
            Version.....................0F
            Configration ID.............01

        Device Id(2)
            Version.....................0F
            Configration ID.............01

        Device Id(3)
            Version.....................0F
            Configration ID.............01

        Device Id(4)
            Version.....................0F
            Configration ID.............01

        Device Id(5)
            Version.....................0F
            Configration ID.............01

        Device Id(6)
            Version.....................0F
            Configration ID.............01
```

```
        Device Id(7)
            Version.....................0F
            Configration 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 ID.........................17:00.0
        Product Name..................HL-325L
        Model Number..................F08GL0DIG017A
        Serial Number.................AO40020264
        Module ID.....................0
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V193-04-04-05

    Device ID.........................17:00.0
        Product Name..................HL-325L
        Model Number..................F08GL0DIG017A
        Serial Number.................AO40020264
        Module ID.....................0
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V193-04-04-05

    Device ID.........................2c:00.0
        Product Name..................HL-325L
        Model Number..................F08GL0DIG017A
```

```
        Serial Number..................AO47046910
        Module ID......................1
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type....................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V491-05-10-07

    Device ID..........................2c:00.0
        Product Name....................HL-325L
        Model Number....................F08GL0DIG017A
        Serial Number..................AO47046910
        Module ID......................1
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type....................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V491-05-10-07

    Device ID..........................3d:00.0
        Product Name....................HL-325L
        Model Number....................F08GL0DIG017A
        Serial Number..................AO47046398
        Module ID......................2
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type....................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V193-20-07-08

    Device ID..........................3d:00.0
        Product Name....................HL-325L
```

```
        Model Number...................F08GL0DIG017A
        Serial Number..................AO47046398
        Module ID......................2
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V193-20-07-08

    Device ID..........................4e:00.0
        Product Name...................HL-325L
        Model Number...................F08GL0DIG017A
        Serial Number..................AO45038496
        Module ID......................3
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V001-02-06-06

    Device ID..........................4e:00.0
        Product Name...................HL-325L
        Model Number...................F08GL0DIG017A
        Serial Number..................AO45038496
        Module ID......................3
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V001-02-06-06

    Device ID..........................97:00.0
```

```
        Product Name...................HL-325L
        Model Number...................F08GL0DIG017A
        Serial Number..................AO45023302
        Module ID......................4
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type....................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V863-02-09-07

    Device ID..........................97:00.0
        Product Name...................HL-325L
        Model Number...................F08GL0DIG017A
        Serial Number..................AO45023302
        Module ID......................4
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type....................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V863-02-09-07

    Device ID..........................a9:00.0
        Product Name...................HL-325L
        Model Number...................F08GL0DIG017A
        Serial Number..................AO47046501
        Module ID......................5
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type....................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V489-19-01-02
```

```
    Device ID.........................a9:00.0
        Product Name..................HL-325L
        Model Number..................F08GL0DIG017A
        Serial Number.................AO47046501
        Module ID.....................5
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V489-19-01-02

    Device ID.........................ba:00.0
        Product Name..................HL-325L
        Model Number..................F08GL0DIG017A
        Serial Number.................AO47046502
        Module ID.....................6
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V491-11-10-05

    Device ID.........................ba:00.0
        Product Name..................HL-325L
        Model Number..................F08GL0DIG017A
        Serial Number.................AO47046502
        Module ID.....................6
        Firmware [SPI] Version..........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version...........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version................Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type.................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version............V0P
        PCB Version.....................R01
        HL Revision.....................1
        AIP UUID........................01P4-0A0903LH-18-U4V491-11-10-05
```

```
    Device ID.........................cb:00.0
        Product Name...................HL-325L
        Model Number...................F08GL0DIG017A
        Serial Number..................AO45052341
        Module ID......................7
        Firmware [SPI] Version.........Preboot version hl-gaudi3-1.20.0-fw-
58.1.1-sec-2 (Feb 13 2025 - 12:01:58)
        Firmware [OS] Version..........Zephyr 2.7.2-hl-gaudi3-1.20.0-fw-58.1.1-
sec-2 (Feb 13 2025 - 12:00:59)
        OAM CPLD Version...............Version: 0x4, Timestamp(epoch):
0x67b607ae [Wed Feb 19 08:32:46 2025]
        OAM Device Type................15D-HBN/15-HBN-MP
        OAM Key Type...................1
        PCB Assembly Version...........V0P
        PCB Version....................R01
        HL Revision....................1
        AIP UUID.......................01P4-0A0903LH-18-U4V234-15-06-01
```

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 OnBoard Retimer System.

```
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
```

The console output contains the following information for Redstone-Next System.

```
Managed system.................196.168.34.56
    HGX Model.................NVIDIA HGX 4-GPU
    FPGA
        version................F.4B
    GPU [1]
        version................96.00.99.00.0D
    GPU [2]
        version................96.00.99.00.0D
    GPU [3]
        version................96.00.99.00.0D
    GPU [4]
        version................96.00.99.00.0D

GPU information
===================
[GPU (1)]
    Location                   : 1
    Model                      : H100 80GB HBM3
    Serial Number              : 1650223014381
    Part Number                : 699-2G520-0202-400
```

```
    Firmware Version           : 96.00.99.00.0D
    GPU GUID                   : 520620b7a35f9e6d2021c711fff2c649
    Board Part Number          : 699-2G520-0202-400
    PCIe Type                  : Gen-1
    Lanes In Use               : -1
    Max Lanes                  : -1
    Memory Vendor              : Unknown
    InfoROM Version            : G520.0202.00.03
    Temperature(C)             : 22 degreeC

[GPU (2)]
    Location                   : 2
    Model                      : H100 80GB HBM3
    Serial Number              : 1650223014049
    Part Number                : 699-2G520-0202-400
    Firmware Version           : 96.00.99.00.0D
    GPU GUID                   : b6668348d52d4f2b2747790a77914d61
    Board Part Number          : 699-2G520-0202-400
    PCIe Type                  : Gen-1
    Lanes In Use               : -1
    Max Lanes                  : -1
    Memory Vendor              : Unknown
    InfoROM Version            : G520.0202.00.03
    Temperature(C)             : 23 degreeC

[GPU (3)]
    Location                   : 3
    Model                      : H100 80GB HBM3
    Serial Number              : 1650223014021
    Part Number                : 699-2G520-0202-400
    Firmware Version           : 96.00.99.00.0D
    GPU GUID                   : b3b7a7ae33c6c238f0d2bb1c927e0708
    Board Part Number          : 699-2G520-0202-400
    PCIe Type                  : Gen-1
    Lanes In Use               : -1
    Max Lanes                  : -1
    Memory Vendor              : Unknown
    InfoROM Version            : G520.0202.00.03
    Temperature(C)             : 23 degreeC

[GPU (4)]
    Location                   : 4
    Model                      : H100 80GB HBM3
    Serial Number              : 1650223014194
    Part Number                : 699-2G520-0202-400
    Firmware Version           : 96.00.99.00.0D
    GPU GUID                   : 21c26a8cd31f18d1b5cee06c5d92eb66
    Board Part Number          : 699-2G520-0202-400
    PCIe Type                  : Gen-1
    Lanes In Use               : -1
    Max Lanes                  : -1
    Memory Vendor              : Unknown
    InfoROM Version            : G520.0202.00.03
```

```
    Temperature(C)             : 23 degreeC

[HGX Redstone System Temperature]
[HBM]
    Reading Temperature        : 31 degreeC
    HBM 1 Temperature          : 30 degreeC
    HBM 2 Temperature          : 29 degreeC
    HBM 3 Temperature          : 31 degreeC
    HBM 4 Temperature          : 28 degreeC
[FPGA]
    Reading Temperature        : 34 degreeC
[GPU Board]
    Reading Temperature        : 28 degreeC
    GPU Board 1 Temperature    : 28 degreeC
    GPU Board 2 Temperature    : 26 degreeC
    GPU Board 3 Temperature    : 27 degreeC
```

The console output contains the following information for GB200 NVL System.

```
Managed system.................196.168.34.56
    HGX Model..................NVIDIA HGX 4-GPU
    HMC
        version................GB200Nvl-24.09-D
        ERoT version...........01.03.0242.0000_n04
    CPLD
        version................0.1C
    CPU [1]
        version................02.03.03
        ERoT version...........01.03.0242.0000_n04
    CPU [2]
        version................02.03.03
        ERoT version...........01.03.0242.0000_n04
    FPGA [1]
        version................1.15
        ERoT version...........01.03.0242.0000_n04
    FPGA [2]
        version................1.15
        ERoT version...........01.03.0242.0000_n04
    GPU  [1]
        version................97.00.40.00.01
        InfoROM version........G548.0201.00.03
    GPU  [2]
        version................97.00.40.00.01
        InfoROM version........G548.0201.00.03
    GPU  [3]
        version................97.00.40.00.01
        InfoROM version........G548.0201.00.03
    GPU  [4]
        version................97.00.40.00.01
        InfoROM version........G548.0201.00.03
```

```
    PCIe Switch Config
        version.................01300524

[HGX GB200 System Informaion]
[Chassis 1]
    Name                        : HGX_Chassis_0
    Model                       : GB200 NVL
    Manufacturer                : NVIDIA
    Serial Number               : N/A
    Part Number                 : N/A
    PowerState                  : On
    MaxPowerWatts               : 0 watts
    MinPowerWatts               : 0 watts
    LocationType                : Backplane

[HMC 1]
    Name                        : HGX_BMC_0
    Model                       : GB200 NVL
    Manufacturer                : NVIDIA
    Serial Number               : 1333324082434
    Part Number                 : 699-24764-0001-QS1
    PowerState                  : On
    LocationType                : Slot
    Temperature(C)              : 29.56 degreeC.

[CPLD 1]
    Name                        : HGX_CPLD_0
    Model                       : MAX10 10M08
    Manufacturer                : Intel
    Serial Number               : NA
    Part Number                 : 115-3953-000
    PowerState                  : On
    LocationType                : Embedded

[FPGA 1]
    Name                        : HGX_FPGA_0
    Model                       : NA
    Manufacturer                : NVIDIA
    Serial Number               : NA
    Part Number                 : 115-3916-000
    PowerState                  : On
    MaxPowerWatts               : 0 watts
    MinPowerWatts               : 0 watts
    LocationType                : Embedded

[FPGA 2]
    Name                        : HGX_FPGA_1
    Model                       : NA
    Manufacturer                : NVIDIA
    Serial Number               : NA
    Part Number                 : 115-3916-000
    PowerState                  : On
    MaxPowerWatts               : 0 watts
```

```
    MinPowerWatts              : 0 watts
    LocationType               : Embedded

[CPU 1]
    Name                       : HGX_CPU_0
    Model                      : Grace A02
    Manufacturer               : NVIDIA
    Serial Number              : 0x00000001780CC147040000000BFF8100
    PowerState                 : On
    LocationType               : Embedded
    Temperature(C)             : 34.97 degreeC.

[CPU 2]
    Name                       : HGX_CPU_1
    Model                      : Grace A02
    Manufacturer               : NVIDIA
    Serial Number              : 0x00000001780CC1C31C00000001018080
    PowerState                 : On
    LocationType               : Embedded
    Temperature(C)             : 34.72 degreeC.

[GPU 1]
    Name                       : HGX_GPU_0
    Model                      : GB200
    Manufacturer               : NVIDIA
    Serial Number              : 1653824001364
    Part Number                : 690-2G548-0201-QS1
    PowerState                 : On
    MaxPowerWatts              : 1200 watts
    MinPowerWatts              : 200 watts
    LocationType               : Embedded
    Temperature(C)             : 34 degreeC.
    Temperature1(C) #Headroom  : 58.72 degreeC.
    InterfaceType              : PCIe
    LanesInUse                 : 1
    MaxLanes                   : 16
    MaxPCIeType                : Gen5
    PCIeType                   : Gen4

[GPU 2]
    Name                       : HGX_GPU_1
    Model                      : GB200
    Manufacturer               : NVIDIA
    Serial Number              : 1653824001364
    Part Number                : 690-2G548-0201-QS1
    PowerState                 : On
    MaxPowerWatts              : 1200 watts
    MinPowerWatts              : 200 watts
    LocationType               : Embedded
    Temperature(C)             : 34 degreeC.
    Temperature1(C) #Headroom  : 57.09 degreeC.
    InterfaceType              : PCIe
    LanesInUse                 : 1
```

```
    MaxLanes                    : 16
    MaxPCIeType                 : Gen5
    PCIeType                    : Gen4

[GPU 3]
    Name                        : HGX_GPU_2
    Model                       : GB200
    Manufacturer                : NVIDIA
    Serial Number               : 1654024000895
    Part Number                 : 690-2G548-0201-QS1
    PowerState                  : On
    MaxPowerWatts               : 1200 watts
    MinPowerWatts               : 200 watts
    LocationType                : Embedded
    Temperature(C)              : 32 degreeC.
    Temperature1(C) #Headroom   : 57.53 degreeC.
    InterfaceType               : PCIe
    LanesInUse                  : 1
    MaxLanes                    : 16
    MaxPCIeType                 : Gen5
    PCIeType                    : Gen4

[GPU 4]
    Name                        : HGX_GPU_3
    Model                       : GB200
    Manufacturer                : NVIDIA
    Serial Number               : 1654024000895
    Part Number                 : 690-2G548-0201-QS1
    PowerState                  : On
    MaxPowerWatts               : 1200 watts
    MinPowerWatts               : 200 watts
    LocationType                : Embedded
    Temperature(C)              : 33 degreeC.
    Temperature1(C) #Headroom   : 58.09 degreeC.
    InterfaceType               : PCIe
    LanesInUse                  : 1
    MaxLanes                    : 16
    MaxPCIeType                 : Gen5
    PCIeType                    : Gen4

[GPU IRot1]
    Name                        : HGX_IRoT_GPU_0
    Manufacturer                : NVIDIA
    Serial Number               : 0xDF88A2EBEC584E5B
    LocationType                : Embedded

[GPU IRot2]
    Name                        : HGX_IRoT_GPU_1
    Manufacturer                : NVIDIA
    Serial Number               : 0xAAAE5844E6184FA9
    LocationType                : Embedded

[GPU IRot3]
```

```
    Name                        : HGX_IRoT_GPU_2
    Manufacturer                : NVIDIA
    Serial Number               : 0x4C79D1E79B04B110
    LocationType                : Embedded

[GPU IRot4]
    Name                        : HGX_IRoT_GPU_3
    Manufacturer                : NVIDIA
    Serial Number               : 0x52A058D24D57098C
    LocationType                : Embedded
```

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
            Configration ID.............01

        Device Id(1)
            Version.....................0F
            Configration ID.............01

        Device Id(2)
            Version.....................0F
            Configration ID.............01

        Device Id(3)
            Version.....................0F
            Configration ID.............01

        Device Id(4)
            Version.....................0F
            Configration ID.............01

        Device Id(5)
            Version.....................0F
            Configration ID.............01

        Device Id(6)
            Version.....................0F
            Configration ID.............01

        Device Id(7)
            Version.....................0F
            Configration 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.....................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:

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

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

Multiple Systems OOB:

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

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l IP_ADDR_RANGE.txt -c GetGpuInfo --
remote_saa /root/saa
```

```
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 IP_ADDR_RANGE.txt -c GetGpuInfo --
remote_saa /root/saa
```

```
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 “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. *Supermicro - 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/HGX_FPGA/HGX_FPGA_EROT/HGX_HMC/HGX_HMC_EROT/HGX_PCIESWITCH/HGX_PCIESWITCH_EROT/HGX_GPU/HGX_GPU_EROT/HGX_NVSWITCH/HGX_NVSWITCH_EROT/HGX_RETIMER/Intel_Gaudi2/Intel_Gaudi3/IntelPVC/MGX GPU/MI300X/ONBOARD_RETIMER/HGX_NVLINKMANAGEMENTNIC/HGX_NVLINKMANAGEMENTNIC_EROT/HGX_GPU_INFOROM/HGX_CPLD/HGX_CPU/HGX_CPU_EROT) to update the GPU firmware of a managed system by SAA.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateGpu --item <CEC|FPGA|HGX|HGX_FPGA|HGX_FPGA_EROT|HGX_HMC|HGX_HMC_EROT|HGX_PCIESWITCH|HGX_PCIESWITCH_EROT|HGX_GPU|HGX_GPU_EROT|HGX_NVSWITCH|HGX_NVSWITCH_EROT|HGX_RETIMER|PVC_RETIMER|GAUDI_RETIMER|PVC_AMC|PVC_UBB_CPLD|MGX_GPU|MI300X|ONBOARD_RETIMER|HGX_NVLINKMANAGEMENTNIC|HGX_NVLINKMANAGEMENTNIC_EROT|GAUDI_UBB_CPLD|GAUDI_UBB_CPLD2|HGX_GPU_INFOROM|HGX_CPLD|HGX_CPU|HGX_CPU_EROT > --file <filename> [--reboot] [--post_complete] [--dev_id <device ID>]
In-Band	saa -I Redfish_HI -u <username> -p <password>-c UpdateGpu --item <CEC|FPGA|HGX|HGX_FPGA|HGX_FPGA_EROT|HGX_HMC|HGX_HMC_EROT|HGX_PCIESWITCH|HGX_PCIESWITCH_EROT|HGX_GPU|HGX_GPU_EROT|HGX_NVSWITCH|HGX_NVSWITCH_EROT|HGX_RETIMER|PVC_RETIMER|GAUDI_RETIMER|PVC_AMC|GAUDI_UBB_CPLD|GAUDI_UBB_CPLD2|MI300X|ONBOARD_RETIMER|HGX_NVLINKMANAGEMENTNIC|HGX_NVLINKMANAGEMENTNIC_EROTHGX_GPU_INFOROM|HGX_CPLD|HGX_CPU|HGX_CPU_EROT> --file <filename> [--reboot] [--dev_id <device ID>] for Intel Gaudi 2 saa -c UpdateGpu --item < GAUDI_OAM_CPLD|GAUDI_SPI|GAUDI_UBB_CPLD > --file <filename> [--reboot] [--dev_id <device ID>] for Intel Gaudi 3 saa -c UpdateGpu --item < GAUDI_OAM_CPLD|GAUDI_SPI > --file <filename> [--reboot] [--dev_id <device ID>] for Intel PVC

	saa -c UpdateGpu --item < PVC_IFWI|PVC_PSCBIN > --file <filename> [--reboot] --dev_id <device ID>
Remote In-Band	saa -l Remote_RHI -u <username> -p <password>} --oi <OS IP address> --ou <OS username> --op <OS password>-c UpdateGpu --item <CEC|FPGA|HGX|HGX_FPGA|HGX_FPGA_EROT|HGX_HMC|HGX_HMC_EROT|HGX_PCIESWITCH|HGX_PCIESWITCH_EROT|HGX_GPU|HGX_GPU_EROT|HGX_NVSWITCH|HGX_NVSWITCH_EROT|HGX_RETIMER|PVC_RETIMER|GAUDI_RETIMER|PVC_AMC|GAUDI_UBB_CPLD|GAUDI_UBB_CPLD2|MI300X|ONBOARD_RETIMER|HGX_NVLINKMANAGEMENTNIC|HGX_NVLINKMANAGEMENTNIC_EROTHGX_GPU_INFOROM|HGX_CPLD|HGX_CPU|HGX_CPU_EROT> --file <filename> [--reboot] [--dev_id <device ID>] for Intel Gaudi 2 saa -l Remote_INB --oi <IP address> --ou <username> --op <password> -c UpdateGpu --item < GAUDI_OAM_CPLD|GAUDI_SPI|GAUDI_UBB_CPLD > --file <filename>[--reboot] [--dev_id <device ID>] for Intel Gaudi 3 saa -l Remote_INB --oi <IP address> --ou <username> --op <password> -c UpdateGpu --item < GAUDI_OAM_CPLD|GAUDI_SPI > --file <filename> [--dev_id <device ID>] [--reboot] for Intel PVC saa -l Remote_INB --oi <IP address> --ou <username> --op <password> -c UpdateGpu --item < PVC_IFWI|PVC_PSCBIN > --file <filename> [--reboot] --dev_id <device ID> [--remote_saa <remote saa_location>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateGpu {--item <CEC|FPGA|HGX|HGX_FPGA|PVC_RETIMER|GAUDI_RETIMER|PVC_AMC|PVC_UBB_CPLD|MGX_GPU|MI300X|HGX_RETIMER|ONBOARD_RETIMER|GAUDI_UBB_CPLD|GAUDI_UBB_CPLD2> --file <filename>} [--reboot [--post_complete]] [--dev_id <device ID>]
Remote In-Band	saa -l Remote_RHI -l <system list file> -c UpdateGpu --item <CEC|FPGA|HGX|HGX_FPGA|HGX_FPGA_EROT|HGX_HMC|HGX_HMC_EROT|HGX_PCIESWITCH|HGX_PCIESWITCH_EROT|HGX_GPU|HGX_GPU_EROT|HGX_NVSWITCH|HGX_NVSWITCH_EROT|H

	GX_RETIMER|PVC_RETIMER|GAUDI_RETIMER|PVC_AMC|GAUDI_UBB_CPLD|GAUDI_UBB_CPLD2MI300X|ONBOARD_RETIMER|HGX_NVLINKMANAGEMENTNIC|HGX_NVLINKMANAGEMENTNIC_EROTHGX_GPU_INFOROM|HGX_CPLD|HGX_CPU|HGX_CPU_EROT> --file <filename> [--reboot] [--dev_id <device ID>] for Intel Gaudi 2 saa -I Remote_INB -l <system list file> -c UpdateGpu --item < GAUDI_OAM_CPLD|GAUDI_SPI|GAUDI_UBB_CPLD > --file <filename> [--reboot] [--dev_id <device ID>] for Intel Gaudi 3 saa -I Remote_INB -l <system list file> -c UpdateGpu --item < GAUDI_OAM_CPLD| GAUDI_SPI > --file <filename> [--reboot][--dev_id <device ID>] for Intel PVC saa -I Remote_INB -l <system list file> -c UpdateGpu --item < PVC_IFWI|PVC_PSCBIN > --file <filename> [--reboot] --dev_id <device ID> [--remote_saa <remote saa_location>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateGpu --
file GPU_CEC.bin --item CEC
```

The console output contains the following information of HGX A100 CEC

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
Managed system.............192.168.34.56
     HGX Model.............HGX A100
   CEC version.............4.0
  FPGA version.............3.03
Local GPU CEC image file......GPU_CEC.bin
Status: Start updating CEC for 192.168.34.56
**********************************WARNING**************************
    Do not remove AC power from the server.
*******************************************************************
Uploading GPU CEC FW...Done
Updating GPU CEC FW ...>>>
```

```
Status: GPU CEC is updated for 192.168.34.56
Note: You have to reboot or power up the system for the changes to take effect
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateGpu --
file NVDIA_HGX_H100.pkg --item HGX --reboot --post_complete
```

The console output contains the following information of HGX H100

```
SuperServer Automation Assistant 1.0.0 (2023/08/18) (x86_64)
Copyright(C) 2023 Super Micro Computer, Inc. All rights reserved.
Managed system.................192.168.34.56
    HGX Model.................HGX H100 8-GPU
    HMC
        version................HGX-22.10-1-rc31
        ERoT version...........00.02.0120.0000_n00
//** Please refer to Note 2 **//
Local GPU image file.........../home/user/GPU/nvfw_HGX-
H100x8_0002_221216.1.0_prod-signed.fwpkg

Status: Start updating HGX for 192.168.34.56

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

Uploading HGX FW.............................
.............Done

Updating HGX FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done
................................
Status: HGX 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
```

[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

The console output contains the following information of PVC_Retimer

```
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
```

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateGpu --file MI300X.pldm --item MI300X --reboot

The console output contains the following information of MI300X

```
Managed system.................. 192.168.34.68
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
Local GPU MI300X image file.............MI300X.pldm
    GPU MI300X image file version.......BKC_X23.44.09
.
Status: Start updating MI300X for 192.168.34.68

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


Uploading MI300X FW.....................
................................................
................................................
.......................Done

Updating MI300X
FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done

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.
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateGpu --
item onboard_retimer --file pt516_x16_reversed_v2_7_0.bin
```

The console output contains the following information of Onboard Retimer

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

Status: Start updating OnBoard Retimer for 192.168.34.56

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


Uploading OnBoard Retimer FW..........
Managed system.................192.168.34.56
    Local Firmware File.................pt516_x16_reversed_v2_7_0.bin
        Version.......................2.7.0
```

```
    OnBoard_Retimer_1..................
        Dev_ID.........................1
        Version........................2.3.0
        Updating FW...>>>
```

```
[SAA_HOME]# ./saa -i 10.141.176.170 -u ADMIN -p ADMIN -c updategpu --item
gaudi_ubb_cpld --file HLB-325_Primary_R0A_20240611a_FPGA_00_0c_RevD.svf
```

The console output contains the following information of Gaudi UBB CPLD

```
SuperServer Automation Assistant 1.1.0_alpha_GD3 (2024/08/02) (x86_64)
Copyright(C) 2024 Super Micro Computer, Inc. All rights reserved.
....

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

Status: Start updating Gaudi 3 UBB CPLD for 10.141.176.170

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


Uploading Gaudi 3 UBB CPLD FW.......

Updating Gaudi 3 UBB CPLD FW.........................................
................................................
................................................
................................................
................................................
................................................
...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>.........>>>>>Done
Done

Updating Gaudi 3 UBB CPLD
FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done

Status: Gaudi 3 UBB CPLD is updated for 10.141.176.170
```

In-Band:

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateGpu --file GPU_FPGA.bin --item FPGA

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateGpu --file NVDIA_HGX_H100.pkg --item HGX --reboot

[SAA_HOME]# ./saa -c updategpu --dev_id 1 --file

HL225_PFR_20230427_0F_644A7EDA_production.signed_cfg0.svf --item GAUDI_OAM_CPLD

The console output contains the following information of 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-LFMXO5-15D-03-TS66530567.itb`

The console output contains the following information of GAUDI OAM CPLD

```
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-LFMXO5-15D-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`

The console output contains the following information of PVC UBB 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 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`

The console output contains the following information of Gaudi SPI

```
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`

The console output contains the following information of Gaudi SPI

```
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..............AO15019764
            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..............AO15019708
            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..............AO15019836
            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..............AO15019755
            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..............AO15019768
            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..............AO15019860
            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..............AO15019869
            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..............AO15019865
```

```
            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_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c UpdateGpu –-dev_id 0 --item PVC_UBB_CPLD --file Etron_UBB-
SA_CPLD1_A02.jed --remote_saa root/saa
```

The console output contains the following information of PVC UBB 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 UBB CPLD
................................................
..
Done.
```

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c UpdateGpu --item PVC_UBB_CPLD --file Etron_UBB-
SA_CPLD1_A02.jed --remote_saa /root/saa
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c UpdateGpu --item
HGX --file NVDIA_HGX_H100.pkg
```

```
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 UpdateGpu --dev_id 0 --
item PVC_UBB_CPLD --file Etron_UBB-SA_CPLD1_A02.jed --remote_saa root/saa
```

```
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 UpdateGpu --file
NVDIA_HGX_H100.pkg --remote_saa /root/saa
```

```
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 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, AMD MI300X, GB200/B200 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 System.
- The vBIOS is the essential firmware that initializes and manages the NVIDIA MGX GPU system, and users can using the option --item MGX_GPU to process the vBIOS firmware update.
- 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_cpld and gaudi_spi on the Intel Gaudi3 system.

5.12.3. Diagnosing AMD MI250 GPU System Status

Diagnoses the AMD MI250 GPU status of the managed system.

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>]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c DiagGpuStatus [--dev_id <dev_id_list>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c DiagGpuStatus [--dev_id <dev_id_list>]
Remote In-Band	saa -I Remote_RHI -l <system list file> -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
```

Remote In-Band:

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

Multiple Systems OOB:

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

```
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 DiagGpuStatus --
remote_saa /root/saa
```

```
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 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

Gets the GPU log of the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetGpuLog --item <HGX [--type DebugToken] | MI300X> --file <file name> [--overwrite]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetGpuLog --item <HGX [--type DebugToken] | MI300X> --file <file name> [--overwrite]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> GetGpuLog --item <HGX [--type DebugToken] | MI300X> --file <file name> [--overwrite]

Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetGpuLog --item <HGX [--type DebugToken] | MI300X> --file <file name> [--overwrite]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetGpuLog --item <HGX [--type DebugToken] | MI300X> --file <file name> [--overwrite]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetGpuLog --item HGX --file log.tgz

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GetGpuLog --item HGX --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 --file log.tgz

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

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c GetGpuLog --item HGX --file log.tgz --overwrite --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c GetGpuLog --item MI300X --file log.tgz --overwrite --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c GetGpuLog --item HGX --type DebugToken --file DebugToken.log --remote_saa /root/saa
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c GetGpuLog --item HGX --file log.tgz

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

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetGpuLog --item HGX --
file log.tgz --overwrite--remote_saa /root/saa
```

```
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 "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.

5.12.5. Getting and Setting GPU Power Limit of the managed system

Gets/Sets the GPU power limit of the managed system.

Command Options	Descriptions
--action	Sets action to: 1 = GetPowerLimit 2 = SetPowerLimit

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GpuPowerManage --item HGX --action <action> [--dev_id <dev_id_list> | ALL] [--value <value>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GpuPowerManage --item HGX --action <action> [--dev_id <dev_id_list> | ALL] [--value <value>]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GpuPowerManage --item HGX --action <action> [--dev_id <dev_id_list> | ALL] [--value <value>]

Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GpuPowerManage --item HGX --action <action> [--dev_id <dev_id_list> | ALL] [--value <value>]
Remote In-Band	saa -l Remote_RHI -l <system list file> -c GpuPowerManage --item HGX --action <action> [--dev_id <dev_id_list> | ALL] [--value <value>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GpuPowerManage
--item HGX --action GetPowerLimit --dev_id 1,2,3
```

The console output contains the following information for HGX.

```
[GPU SXM 1]
    Power Limit Max value: 700
    Power Limit Min value: 200
    Power Limit Current value: 700

[GPU SXM 2]
    Power Limit Max value: 700
    Power Limit Min value: 200
    Power Limit Current value: 700

[GPU SXM 3]
    Power Limit Max value: 700
    Power Limit Min value: 200
    Power Limit Current value: 700
```

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c GpuPowerManage
--item HGX --action SetPowerLimit --dev_id 1,2,3 --value 700
```

The console output contains the following information for HGX.

```
.............................
Set GPU SXM 1,2,3 Power Limit successfully.
```

In-Band:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GpuPowerManage --item HGX --action SetPowerLimit --dev_id all

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c GpuPowerManage --item HGX --action SetPowerLimit --dev_id all --value 700
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c GpuPowerManage --item HGX --action GetPowerLimit --remote_saa /root/saa

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c GpuPowerManage --item HGX --action SetPowerLimit --value 700 --dev_id 1,2,3 --remote_saa /root/saa
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p ADMIN -c GpuPowerManage --item HGX --action GetPowerLimit
```

```
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 GpuPowerManage --item HGX --action GetPowerLimit --remote_saa /root/saa
```

```
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 "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]] [--json_view]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetCpldInfo [--file <filename> [--file_only] [--extract_measurement]] [--json_view]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetCpldInfo [--file <filename> [--file_only] [--extract_measurement]] [--json_view] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetCpldInfo [--file <filename> [--extract_measurement]] [--json_view]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetCpldInfo [--file <filename>] [--remote_saa <remote SAA path>] [--json_view]

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
```

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 GetCpldInfo --file CPLD.bin
```

```
[SAA_HOME]# ./saa -I Remote_RHI -u ADMIN -p PASSWORD --oi 192.168.34.56 -
-ou root --op 111111 -c GetCpldInfo
```

Multiple Systems OOB:

```
[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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetCpldInfo --file
CPLD.bin

[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetCpldInfo
```

```
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 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
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateCpld --file <filename> [--index <num>] --reboot [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateCpld --file <filename> [--index <num>] --reboot
Remote In-Band	saa -I Remote_RHI -l <system list file> -c UpdateCpld --file <filename> --reboot [--remote_saa <remote SAA path>]

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
```

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 UpdateCpld --file CPLD.bin
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c UpdateCpld --file
CPLD.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.



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 [--file <filename>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetSwitchboardCpldInfo [--file <filename> [--file_only]]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetSwitchboardCpldInfo [--file <filename>] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetSwitchboardCpldInfo [--file <filename>]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetSwitchboardCpldInfo [--file <filename>] [--remote_saa <remote SAA path>]

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	*It is possible to install many left switchboards.* Left switchboard only can be displayed if the system has fully boot up.
Right Switchboard	*It is possible to install many right switchboards.* 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 [--post_complete]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateSwitchboardCpld --file <filename> --type <type> [--index <index>] [--reboot]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateSwitchboardCpld --file <filename> --type <type> [--index <index>] [--reboot] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateSwitchboardCpld --file <filename> --type <type> [--index <index>] [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c UpdateSwitchboardCpld --file <filename> --type <type> [--index <index>] [--reboot] [--remote_saa <remote SAA path>]

Example:

OOB:

```
[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 OOB:

```
[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 [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetBackplaneCpldInfo [--json_view]
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 GetBackplaneCpldInfo [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBackplaneCpldInfo [--json_view]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c GetBackplaneCpldInfo [--json_view]

Example:

OOB:

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

The console output contains the following information.

```
Managed system.......................192.168.34.56
    [Backplane 1]
```

```
        CPLD 1 ID.....................0023
        CPLD 1 version.................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.

```
Managed system.......................169.254.3.254
    [Backplane 1]
        CPLD 1 ID.....................0023
        CPLD 1 version.................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.



Notes:

- Backplane and CPLD index numbers may not be displayed if they are not supported by the managed system.

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.

Single System

OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateBackplaneCpld [{--index <BPN index> --file <filename> | --update_list <BPN index>:<filename>[,<BPN index>:<filename>...]}] [--reboot] --manual_ejected
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateBackplaneCpld [{--index <BPN index> --file <filename> | --update_list <BPN index>:<filename>[,<BPN index>:<filename>...]}] [--reboot] --manual_ejected
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 UpdateBackplaneCpld [{--index <BPN index> --file <filename> | --update_list <BPN index>:<filename>[,<BPN index>:<filename>...]}] [--reboot] --manual_ejected
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateBackplaneCpld [{--index <BPN index> --file <filename> | --update_list <BPN index>:<filename>[,<BPN index>:<filename>...]}] [--reboot] --manual_ejected
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c UpdateBackplaneCpld [{--index <BPN index> --file <filename> | --update_list <BPN index>:<filename>[,<BPN index>:<filename>...]}] [--reboot] --manual_ejected

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateBackplaneCpld --index 0 --file BPN_CPLD.jed --manual_ejected
```

The console output contains the following information.

```
Status: Start updating Backplane CPLD for 192.168.34.56

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

Warning: All drives on backplane will be force ejected due to backplane reset
after update.
```

```
Managed system.....................192.168.34.56
    [Backplane 1]
        CPLD 1 ID..................0023
        CPLD 1 version.............0C
Local CPLD image file..............BPN_CPLD.jed

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

Status: Backplane CPLD is updated for 192.168.34.56
```

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateBackplaneCpld --update_list 0:BPN_CPLD.jed,1:BPN_CPLD.jed --
manual_ejected
```

The console output contains the following information.

```
Status: Start updating Backplane CPLD for 192.168.34.56

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

Warning: All drives on backplane will be force ejected due to backplane reset
after update.

Managed system.....................192.168.34.56
    Backplane CPLD ID..............0023
    Backplane CPLD Revision.........0C
    Local CPLD image file..............BPN_CPLD.jed
    Uploading FW...Done
    Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>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.



Notes:

- This command is only available on systems with storage backplanes installed.
- Backplane and CPLD index numbers may not be displayed if they are not supported by the managed system.

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 [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetFanboardCpldInfo [--json_view]
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 GetFanboardCpldInfo [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetFanboardCpldInfo [--json_view]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c GetFanboardCpldInfo [--json_view]

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.............................169.254.3.254
    [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>]
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 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>]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -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.

```
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
```



Note:
This command is supported on the SYS-420GH-TNGR system.

Example:

OOB:

```
[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.

```
Managed system.....................192.168.34.56
    AIP FW version.................1A;1A;1A;1A;1A;1A;1A;1A
Local AIP image file...............AIP_CPLD.bin

Status: Start updating AIP CPLD for 192.168.34.56

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

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

Status: AIP CPLD is updated for 192.168.34.56
Update Complete, Please wait for BMC reboot, about 5 mins.
................................................
................................................
................................................
................................................
................................................
.............................................Done
```

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 [--file <filename>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetAomboardCpldInfo [--file <filename> [--file_only]]
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 GetAomboardCpldInfo [--file <filename> [--file_only]] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetAomboardCpldInfo [--file <filename>]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c GetAomboardCpldInfo [--file <filename>] [--remote_saa <remote SAA path>]

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>] [--index <id>] [--aom_type <type>] [--reboot [--post_complete]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateAomboardCpld --file <filename> [--dev_id <id>] [--index <id>] [--aom_type <type>] [--reboot]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateAomboardCpld --file <filename> [--dev_id <id>] [--index <id>] [--aom_type <type>] [--reboot] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateAomboardCpld --file <filename> [--dev_id <id>] [--index <id>] [--aom_type <type>] [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c UpdateAomboardCpld --file <filename> [--dev_id <id>] [--index <id>] [--aom_type <type>] [--reboot] [--remote_saa <remote SAA path>]

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
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetMiscCpldInfo [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l < system list file > [-u <username> -p <password>] -c GetMiscCpldInfo
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetMiscCpldInfo [--remote_saa <remote SAA path>]

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
```

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 GetMiscCpldInfo
```

Multiple Systems OOB:

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

```
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 GetMiscCpldInfo
```

```
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 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.

Single System	
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
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateMiscCpld --file <filename> --reboot [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMiscCpld --file <filename> --reboot
Remote In-Band	saa -I Remote_RHI -l <system list file> -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
```

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 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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c UpdateMiscCpld --file
MISC_CPLD.jed --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
```

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
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetMidplaneSbbCpldInfo [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetMidplaneSbbCpldInfo
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetMidplaneSbbCpldInfo [--remote_saa <remote SAA path>]

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	saa -i <IP or host name> -u <username> -p <password> -c UpdateMidplaneSbbCpld --file <filename> --index <id> --reboot [--post_complete]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateMidplaneSbbCpld --file <filename> --index <id> --reboot
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateMidplaneSbbCpld --file <filename> --index <id> --reboot [--remote_saa <remote SAA path>]

Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMidplaneSbbCpld --file <filename> --index <id> --reboot [--post_complete]
Remote In-Band	saa -l Remote_RHI -l <system list file> -c UpdateMidplaneSbbCpld --file <filename> --index <id> --reboot [--remote_saa <remote SAA path>]

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.

```
Managed system.....................192.168.34.56
    Midplane SBB CPLD 1 version....CPLD_ID: 0000 REV: 02
Local CPLD image file..............MidplaneSBB_CPLD.jed

Status: Start updating Midplane SBB CPLD for 192.168.34.56

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

Uploading FW...Done

Preparing updating..................Done

Updating FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done

Rebooting target system.............................................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


Status: Midplane SBB CPLD is updated for 192.168.34.56
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
UpdateMidplaneSbbCpld --file MidplaneSBB_CPLD.jed --index 1 --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.



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
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetNICCpldInfo [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c

	GetNICCpldInfo
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetNICCpldInfo [--remote_saa <remote SAA path>]

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 AOC-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 AOC-A200G-B2CM
            CPLD ID...........32E8
            CPLD Rev..........02
```

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 GetNICCpldInfo
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetNICCpldInfo
```

```
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
```

5.13.18 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 -I Redfish_HI -c UpdateNICCpld --file <filename> [--dev_id <Device ID>]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateNICCpld --file <filename> [--dev_id <Device ID>][--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateNICCpld --file <filename> [--dev_id <Device ID>] [--individually]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c UpdateNICCpld --file <filename> [--remote_saa <remote SAA path>]

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
```

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 UpdateNICCpld --file NIC_CPLD.jed
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c UpdateNICCpld --file
NIC_CPLD.jed
```

```
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
```

5.13.19. 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 [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetTransitionboardCpldInfo [--json_view]
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 GetTransitionboardCpldInfo [--json_view]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetTransitionboardCpldInfo [--json_view]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c GetTransitionboardCpldInfo [--json_view]

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	
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 UpdateTransitionboardCpld --file <filename>
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateTransitionboardCpld --file <filename>
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -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:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
UpdateTransitionboardCpld --file Transboard_CPLD.jed
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
UpdateTransitionboardCpld --file Transboard_CPLD.jed
```

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

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateTransitionboardCpld --file Transboard_CPLD.jed
```

The console output contains the following information.

```
Managed system.....................192.168.34.56
    CPLD version...................00.00.00

Status: Start updating Transitionboard 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: Transitionboard CPLD is updated for 192.168.34.56

Note: Update done. No further action is needed for this firmware to take effect.
```

Multiple Systems OOB:

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

5.14. 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 <dev_id_list>]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetAocNICInfo [--file <filename>] [--file_only] [--dev_id <dev_id_list>]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetAocNICInfo [--file <filename>] [--file_only] [--dev_id <dev_id_list>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetAocNICInfo [--file <filename>] [--file_only] [--dev_id <dev_id_list>]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetAocNICInfo [--file <filename>] [--file_only] [--dev_id <dev_id_list>]

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)
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c GetAocNICInfo --dev_id 1,2,3 --file AOC_NIC.bin --
remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetAocNICInfo --dev_id
1,2,3 --file AOC_NIC.bin --remote_saa /root/saa
```

```
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 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> [--upgrade_only] [[--reboot [--post_complete]] | [--check_reboot_required]]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c UpdateAocNIC {--file <filename> --dev_id <add-on NIC device ID>} [--upgrade_only] [[--reboot] | [--check_reboot_required]]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateAocNIC {--file <filename> --dev_id <add-on NIC device ID>} [--upgrade_only] [[--reboot] | [--check_reboot_required]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateAocNIC {--file <filename> --dev_id <add-on NIC device ID> [--upgrade_only] [[--reboot [--post_complete]] | [--check_reboot_required]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c UpdateAocNIC {--file <filename> --dev_id <add-on NIC device ID>} [--upgrade_only] [[--reboot] | [--check_reboot_required]]

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

[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateAocNIC --file AOC_NIC.bin --dev_id 1 --upgrade_only --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

[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c UpdateAocNIC --file AOC_NIC.bin --dev_id 1 --check_reboot_required
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c UpdateAocNIC --file AOC_NIC_FW.rom --dev_id 2 --
reboot --remote_saa /root/saa
```

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c UpdateAocNIC --file AOC_NIC_FW.rom --dev_id 2 --
reboot --upgrade_only --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c UpdateAocNIC --file
AOC_NIC_FW.rom --dev_id 2 --reboot --remote_saa /root/saa
```

```
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 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.

The GetTpInfo command can obtain the the following informations.

1. The information for each node, which contains **Power status, IP, DC output power, DC output current, CPU temperature, node PN, and node SN**.

2. The current node information, which includes read-only information and configurable settings:

- Information: **Backplane revision, Backplane ID, TwinPro type and MCU version**.
- Configuration: **Config ID, System name, System PN, System SN, Chassis PN, Chassis SN, Backplane PN, Backplane SN, Node PN, Node SN, Chassis Location, and Backplane Location**.

For details on TwinPro configuration, refer to ***4.7.7, TwinPro Configuration XML File Format***.

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]]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GetTpInfo [--file <filename> [--overwrite]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetTpInfo [--file <filename> [--overwrite]]
Remote In-Band	saa -I Remote_INB -l <system list file> -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
```

Remote In-Band:

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

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GetTpInfo --file
TpInfo.xml --overwrite
```

```
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 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c ChangeTpInfo --file <filename> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c ChangeTpInfo --file <filename> [--individually]
Remote In-Band	saa -I Remote_INB -l <system list file> -c ChangeTpInfo --file <filename> [--remote_saa <remote SAA path>]

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.



Note:
After changing TP info, if the BMC display does not update, reset the BMC. On certain platforms, a BMC reset is required for TP changes to take effect.

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>] [--json_view]
In-Band	saa [-I Redfish_HI -u <username> -p <password>] -c GetMultinodeEcInfo [--file <filename> [--file_only]] [--json_view]
Remote In-Band	saa {-I Remote_INB | Remote_RHI -u <username> -p <password>} --oi <OS IP address> --ou <OS username> --op <OS password> [--remote_saa <remote SAA path>] -c GetMultinodeEcInfo [--file <filename> [--file_only]] [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetMultinodeEcInfo [--file <filename>] [--json_view]
Remote In-Band	saa -I {Remote_INB | Remote_RHI} -l <system list file> [--remote_saa <remote SAA path>] -c GetMultinodeEcInfo [--file <filename> [--file_only]] [--json_view]

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>
Remote In-Band	saa -I {Remote_INB | Remote_RHI -u <username> -p <password>} --oi <OS IP address> --ou <OS username> --op <OS password> [--

	remote_saa <remote SAA path>] -c UpdateMultinodeEc --file <filename>
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMultinodeEc --file <filename>
Remote In-Band	saa -I {Remote_INB | Remote_RHI} -l <system list file> [--remote_saa <remote SAA path>] -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 OOB:

```
[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.

5.15.5. Getting Multi-Node LCMC Firmware Image Information

Use the “GetMultinodeLcmcInfo” command to get the multi-node LCMC firmware image information from the managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c GetMultinodeLcmcInfo [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetMultinodeLcmcInfo [--json_view]
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 GetMultinodeLcmcInfo [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetMultinodeLcmcInfo [--json_view]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c GetMultinodeLcmcInfo [--json_view]

Example:

OOB:

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

In-Band Redfish Host Interface:

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

The console output contains the following information.

```
Managed system.....................169.254.3.254
    LCMC version...................0.07
```

Multiple Systems OOB:

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

```
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.

5.15.6. Updating the Multi-node LCMC Firmware Image

Use the “UpdateMultinodeLcmc” command with the given multi-node LCMC firmware image to run SAA to update the multi-node LCMC firmware of a managed system.

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c UpdateMultinodeLcmc --file <filename> --reboot [--post_complete]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c UpdateMultinodeLcmc --file <filename> --reboot

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateMultinodeLcmc --file <filename> --reboot [--post_complete]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c
UpdateMultinodeLcmc --file LCMC.jed --reboot --post_complete
```

The console output contains the following information.

```
Managed system.....................192.168.34.56
    LCMC version...................0.07

Status: Start updating Multi-node LCMC for 192.168.34.56

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


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

Status: The managed system 192.168.34.56 is waiting for POST complete

..........
Status: OEM

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


Status: Multi-node LCMC is updated for 192.168.34.56
```

In-Band Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Redfish_HI -u ADMIN -p PASSWORD -c
UpdateMultinodeLcmc --file LCMC.jed --reboot
```

Multiple Systems OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c
UpdateMultinodeLcmc --file LCMC.jed --reboot
```

```
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.

5.16. 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><file path> \\<hostname or IP>:<port number><file path> \\<hostname or IP><shared point><file path> \\<hostname or IP>:<port number><shared point><file path>
Share host	<hostname or IP> or <hostname or IP>:<port number>
Path to image	<shared point>/<file path> or <file path>

Allowed character classes:

- a-z
- A-Z
- 0-9
- Special characters for ID and password: ^ (a caret)
- Special characters for a shared host: - (a dash) or . (a period)
- Special character for a shared host in HTTP and SAMBA protocols in an IPv6 URL: : (a colon)
- The shared host for HTTP IPv6 address should be enclosed by square brackets: [ ]
- Special characters for path to image: @,^,-,_,., /, and \ (Note that a slash/ and a backslash \ can only be used in a path.
- Special characters like backslashes \ and slashes / should only be used once; repeated use (e.g., //, \, /\ and /) are not allowed.
- Special character ^ (a caret) is not available for use in older versions of BMC firmware.
- The port number may not be supported in older versions of BMC firmware.
- IPv6 link-local address starts with fe80 is not allowed.

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>]]
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 MountIsoImage --image_url <URL> [[--id <id for URL> --pw <password for URL>] | [--id <id for URL> --pw_file <password file path>]] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <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>]]
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c MountIsoImage --image_url <URL> [[--id <id for URL> --pw <password for URL>] | [--id <id for URL> --pw_file <password file path>]] [--remote_saa <remote SAA 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 smbid --
pw smbpasswd
```

```
[SAA_HOME]# ./saa -c MountIsoImage --image_url
'https://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd

[SAA_HOME]# ./saa -c MountIsoImage --image_url
'https://[2001:db8::1]:80/MySharedPoint/MyFolder/Image.iso' --id smbid --
pw smbpasswd

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

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

```
smbpasswd.txt:
    smbpasswd
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c MountIsoImage --image_url
'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpassword
```

Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c MountIsoImage --image_url
'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpassword
```

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
smbid --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
smbid --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
smbid --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
smbid --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 smbpasswd

[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

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c MountIsoImage --
image_url '\\2001:db8::1\MySharedPoint\MyFolder\Image.iso' --id smbid --
pw_file smbpasswd.txt
```

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

```
smbpasswd.txt:
    smbpasswd
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c MountIsoImage --image_url
'smb://192.168.35.1/MYSharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd
```

```
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 MountIsoImage --image_url
'smb://192.168.35.1/MYSharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd
```

```
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 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 [-I Redfish_HI -u <username> -p <password>] -c UnmountIsoImage
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 UnmountIsoImage [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UnmountIsoImage
Remote In-Band	saa {-I Remote_INB | -I Remote_RHI} -l <system list file> -c UnmountIsoImage [--remote_saa <remote SAA path>]

Example:

OOB:

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

In-Band:

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

Remote In-Band:

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

Remote In-Band through Redfish Host Interface:

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c UnmountIsoImage
```

```
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 UnmountIsoImage
```

```
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 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 -I Redfish_HI -u <username> -p <password> -c GetVmInfo [--dev_id <device ID>]
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetVmInfo [--dev_id <device ID>] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetVmInfo [--dev_id <device ID>]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetVmInfo [--dev_id <device ID>] [--remote_saa <remote SAA path>]

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 through Redfish Host Interface:

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

[SAA_HOME]# ./saa -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
```

Remote In-Band through Redfish Host Interface:

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

[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c GetVmInfo --dev_id 1
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l Slist.txt -c GetVmInfo

[SAA_HOME]# ./saa -I Remote_RHI -l Slist.txt -c GetVmInfo --dev_id 1
```

```
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.

5.16.6. 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	saa -i <IP or host name> -u <username> -p <password> -c VmManage {--action <Enable|Disable> [--port <port>] | --action Mount [--dev_id <device ID>] --image_url <URL> [[--id <id for URL> --pw <password for URL>]|[--id <id for URL> --pw_file <password file path>]] [--verify_cert [--accept_self_signed]] | --action Unmount [--dev_id <device ID>]}
In-Band	saa -I Redfish_HI -u <username> -p <password> -c VmManage {--action <Enable|Disable> [--port <port>] | --action Mount [--dev_id <device ID>] --image_url <URL> [[--id <id for URL> --pw <password for URL>]|[--id <id for URL> --pw_file <password file path>]] [--verify_cert [--accept_self_signed]] | --action Unmount [--dev_id <device ID>]}
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c VmManage {--action <Enable|Disable> [--port <port>] | --action Mount [--dev_id <device ID>] --image_url <URL> [[--id <id for URL> --pw <password for URL>]|[--id <id for URL> --pw_file <password file path>]] [--verify_cert [--accept_self_signed]] | --action Unmount [--dev_id <device ID>]} [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c VmManage {--action <Enable|Disable> [--port <port>] | --action Mount [--dev_id <device ID>] --image_url <URL> [[--id <id for URL> --pw <password for URL>]|[--id <id for URL> --pw_file <password file path>]] [--verify_cert [--accept_self_signed]] | --action Unmount [--dev_id <device ID>]}
Remote In-Band	saa -I Remote_RHI -l <system list file> -c VmManage {--action <Enable|Disable> [--port <port>] | --action Mount [--dev_id <device ID>] --image_url <URL> [[--id <id for URL> --pw <password for URL>]|[--id <id for URL> --pw_file <password file path>]] [--verify_cert [--accept_self_signed]] | --action Unmount [--dev_id <device ID>]} [--remote_saa <remote SAA path>]

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 smbid --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 smbid --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 smbid --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 smbid --
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 smbid --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 smbid --
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 smbid --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 smbid --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 through Redfish Host Interface:

```
[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 smbid --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 smbid --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 smbid --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 smbid --
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 smbid --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 smbid --
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
smbid --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
smbid --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
```

Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111
-u ADMIN -p ADMIN -c VmManage --action Mount --image_url
'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw
smbpasswd --dev_id 1
```

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 smbid --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 smbid --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 smbid --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 smbid --
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 smbid --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 smbid --
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
smbid --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
smbid --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
```

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

```
smbpasswd.txt:
    smbpasswd
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l Slist.txt -c VmManage --action Mount --image_url 'smb://192.168.35.1/MySharedPoint/MyFolder/Image.iso' --id smbid --pw smbpasswd --dev_id 1
```

```
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:

- 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
```

5.16.8. Managing a BMC Host in SAA Shell Mode

Use the “Ch” command to manage the BMC host IP address in SAA shell mode. Before running the "Ch" command, you need to enter SAA shell mode, refer to 5.11.11. Shell Mode for details.

The servers that have been accessed are automatically saved. Next time when you enter the SAA shell mode, the servers will be recalled in the prompt. You can use the "<" or ">" keys to switch between the servers.

Single System	
SAA shell	Ch [{--host_ip <BMC IP> | --index <Host index>} [{[--user_name <BMC username>] [--user_password <BMC user password>] | --remove}]]

Example:

Enter SAA shell mode:

```
[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
Managed hosts loaded.

ADMIN@192.168.34.56 X12SPW X12_RoT_ATEN_AST2600>
```

SAA shell:

```
[SAA_HOME]# X12_ATEN_AST2600> Ch
```

The console output contains the following information.

```
ADMIN@192.168.34.56 X12SPW X12_RoT_ATEN_AST2600> Ch

Current setting:
IP       : 192.168.34.56
Username : ADMIN

Current managed system(s):

 Index | IP              Board            DC Room  Row Rack  Num Type        |
BMC
 ----- | ---------------- -----          ---- ---- ---- ---- ---- ----        | -
------
     1 | 192.168.34.56                                                       |
```

```
      2 | 192.168.34.57                                                                |
      3 | 192.168.34.58                                                                |

Use "ch --index <index> --remove" to remove.
Use "ch" to change or add managed system (IP)
Use "<" or ">" to switch managed system on shell prompt

Usage: ch --host_ip <IP> [--user_name <username>] [--user_password <password>]
Using wild card for IP
ex: 192.168.100.118 change to 192.168.100.9
    CMM>ch *.9



ADMIN@192.168.34.56 X12SPW X12_RoT_ATEN_AST2600>
```

`[SAA_HOME]# X12_ATEN_AST2600> Ch --host_ip 192.168.34.59`

The console output contains the following information.

```
ADMIN@192.168.34.56X12SPW X12_RoT_ATEN_AST2600> Ch --host_ip 192.168.34.59

Old IP       : 192.168.34.56
New IP       : 192.168.34.59

ADMIN@192.168.34.59 X13SEM X13_RoT2.0_ATEN_AST2600_2_1>
```

`[SAA_HOME]# X12_ATEN_AST2600> Ch --index 1`

The console output contains the following information.

```
ADMIN@192.168.34.59 X13SEM X13_RoT2.0_ATEN_AST2600_2_1> ch --index 1
1 -> 192.168.34.56
Old IP       : 192.168.34.59
New IP       : 192.168.34.56

ADMIN@192.168.34.56 X12SPW X12_RoT_ATEN_AST2600>
```

`[SAA_HOME]# X12_ATEN_AST2600> Ch --index 2 --remove`

The console output contains the following information.

```
ADMIN@192.168.34.56 X12SPW X12_RoT_ATEN_AST2600> Ch --index 2 --remove
```

```
192.168.34.57 removed.


ADMIN@192.168.34.56 X12SPW X12_RoT_ATEN_AST2600>
```



Note:
When changing hosts with Ch command without options --use_name or --user_password, SAA will try to log in to the target system with the current login username and password.

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
Description	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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action GetDeviceID [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action GetDeviceID
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action GetDeviceID [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmMeManage --type NM20 --action GetDeviceID --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --
action GetDeviceID --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action Reset [--remote_saa <remote SAA path>]

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action Reset
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action Reset [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmMeManage --type NM20 --action Reset --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --action Reset --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action ResetToDefault [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action ResetToDefault
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action ResetToDefault [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmMeManage --type NM20 --action ResetToDefault --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --
action ResetToDefault --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action EnterToUpdateMode [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action EnterToUpdateMode
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action EnterToUpdateMode [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmMeManage --type NM20 --action EnterToUpdateMode --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --action EnterToUpdateMode --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action PowerOff [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action PowerOff
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action PowerOff [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmMeManage --type NM20 --action PowerOff --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --
action PowerOff --remote_saa /root/saa
```

```
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.

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	saa -i <IP or host name> -u <username> -p <password> -c NmMeManage --type NM20 --action SelfTest
In-Band	saa -c NmMeManage --type NM20 --action SelfTest

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action SelfTest [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action SelfTest
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action SelfTest [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmMeManage --type NM20 --action SelfTest --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --action SelfTest --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action Mode [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action Mode
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action Mode [--remote_saa <remote SAA path>]

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.
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmMeManage --type NM20 --action Mode --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --
action Mode --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action ListImagesInfo [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action ListImagesInfo
Remote In-Band	saa -I Remote_INB -l <system list file>-c NmMeManage --type NM20 --action ListImagesInfo [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmMeManage --type NM20 --action ListImagesInfo --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --
action ListImagesInfo --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action GetPower [--remote_saa <remote SAA path>]

Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action GetPower
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action GetPower [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111-c NmMeManage --type NM20 --action GetPower --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --
action GetPower --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmMeManage --type NM20 --action GetTemp [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c NmMeManage --type NM20 --action GetTemp
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmMeManage --type NM20 --action GetTemp [--remote_saa <remote SAA path>]

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.

```
56 (C)
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmMeManage --type NM20 --action GetTemp --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmMeManage --type NM20 --
action GetTemp --remote_saa /root/saa
```

```
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.

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	GetNMSDR = 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



Note:
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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action GetNMSDR [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetNMSDR
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetNMSDR [--remote_saa <remote SAA path>]

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 -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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action GetNMSDR --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetNMSDR --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action GetSelTime [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetSelTime
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetSelTime [--remote_saa <remote SAA path>]

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 -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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetSelTime --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> GeneralNmManage --type NM20 --action GetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> [--remote_saa <remote SAA path>]
Multiple Systems	
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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type NM20 --action GetStatistics -
-mode 1 --domain_id 0 --policy_id 0
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action GetStatistics --mode 1 --
domain_id 0 --policy_id 0 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetStatistics --mode 1 --domain_id 0 --policy_id 0 --
remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> [--remote_saa <remote SAA path>]
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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type NM20 --action ResetStatistics
--mode 0 --domain_id 0 --policy_id 0
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action ResetStatistics --mode 0 --
domain_id 0 --policy_id 0 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action ResetStatistics --mode 0 --domain_id 0 --policy_id 0 --
remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type> [--remote_saa <remote SAA path>]

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 -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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action GetCapabilities --domain_id 0 --
trigger_type 0 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetCapabilities --domain_id 0 --trigger_type 0 --remote_saa
/root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action GetVersion [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetVersion
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetVersion [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type NM20 --action GetVersion
```

The console output contains the following information.

```
Node Manager Version = 2.0
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action GetVersion --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetVersion --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action GetAlert [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetAlert
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetAlert [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type NM20 --action GetAlert
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action GetAlert --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetAlert --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action SetAlert --value <assignment value> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action SetAlert --value <assignment

	value>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action SetAlert --value <assignment value> [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type NM20 --action SetAlert --
value 1
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action SetAlert --value 1 --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action SetAlert --value 1 --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action GetTotalPower --domain_id <Domain ID> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetTotalPower --domain_id <Domain ID>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetTotalPower --domain_id <Domain ID> [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type NM20 --action GetTotalPower -
-domain_id 0
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action GetTotalPower --domain_id 0 --
remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetTotalPower --domain_id 0 --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action SetTotalPower --domain_id <Domain ID> --value <assignment value> [--remote_saa <remote SAA path>]
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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action SetTotalPower --domain_id <Domain ID> --value <assignment value> [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type NM20 --action SetTotalPower --domain_id 0 --value 100
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c GeneralNmManage --type NM20 --action SetTotalPower --domain_id 0 --value 100 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type NM20 --action SetTotalPower --domain_id 0 --value 100 --remote_saa /root/saa
```

```
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.

5.17.2.1.11. 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 are the supported options for the --action DelTotalPower option.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action DelTotalPower --domain_id <Domain ID> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action DelTotalPower --domain_id <Domain ID>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action DelTotalPower --domain_id <Domain ID> [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action DelTotalPower --domain_id 0 --
remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action DelTotalPower --domain_id 0 --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range> [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type NM20 --action
SetPowerDrawRange --domain_id 0 --range 0-32767
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action SetPowerDrawRange --domain_id 0 -
-range 0-32767 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action SetPowerDrawRange --domain_id 0 --range 0-32767 --
remote_saa /root/saa
```

```
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.

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

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action GetSensor [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetSensor
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetSensor [--remote_saa <remote SAA path>]

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 -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       |
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action GetSensor --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetSensor --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type NM20 --action GetSummary [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type NM20 --action GetSummary
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type NM20 --action GetSummary [--remote_saa <remote SAA path>]

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 -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|
+------------------------------------+
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type NM20 --action GetSummary --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
NM20 --action GetSummary --remote_saa /root/saa
```

```
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.

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 Platform Power (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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action GetSelTime [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action GetSelTime
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action GetSelTime [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action GetSelTime --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action GetSelTime --remote_saa /root/saa
```

```
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.

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 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. 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. 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. 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 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS 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>
Multiple Systems	
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>
Remote In-Band	saa -I Remote_INB -l <system list file> -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> [--remote_saa <remote SAA path>]

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

Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c GeneralNmManage --type BMC10 --action GetStatistics --mode 1 --domain_id 1 --policy_id 1 --per_component_control 0 --component_id 0 --remote_saa /root/saa

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
```

Multiple Systems Remote In-Band:

[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type BMC10 --action GetStatistics --mode 1 --domain_id 1 --policy_id 1 --per_component_control 0 --component_id 0 --remote_saa /root/saa

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> [--remote_saa <remote SAA path>]
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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action ResetStatistics --mode <Mode> --domain_id <Domain ID> --policy_id <Policy ID> [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type BMC10 --action
ResetStatistics --mode 1 --domain_id 1 --policy_id 1
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action ResetStatistics --mode 1 --
domain_id 1 --policy_id 1 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action ResetStatistics --mode 1 --domain_id 1 --policy_id 1 --
remote_saa /root/saa
```

```
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.

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>

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type> [--remote_saa <remote SAA path>]
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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action GetCapabilities --domain_id <Domain ID> --trigger_type <Trigger Type> [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action GetCapabilities --domain_id 1 --
trigger_type 0 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action GetCapabilities --domain_id 1 --trigger_type 0 --
remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action GetVersion [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action GetVersion
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action GetVersion [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type BMC10 --action GetVersion
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action GetVersion --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action GetVersion --remote_saa /root/saa
```

```
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.

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. 0 - Power budget should be applied to whole domain (persistent setting). 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 PECI 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 PECI 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action GetTotalPower --domain_id <Domain ID> --per_component_control

	<Per-component Control> --component_id <Component ID> [--remote_saa <remote SAA path>]
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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action GetTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID> [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action GetTotalPower --domain_id 0 --
per_component_control 1 --component_id 0 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action GetTotalPower --domain_id 0 --per_component_control 1 --
component_id 0 --remote_saa /root/saa
```

```
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.

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. 0 - Power budget should be applied to whole domain (persistent setting). 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 PECI 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 PECI 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 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id <Domain ID> --value <assignment value> --per_component_control <Per-component Control> --component_id <Component ID> [--remote_saa <remote SAA path>]
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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id <Domain ID> --value <assignment value> --per_component_control <Per-component Control> --component_id <Component ID> [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type BMC10 --action SetTotalPower
--domain_id 0 --value 100 --per_component_control 1 --component_id 0
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action SetTotalPower --domain_id 0 --
value 100 --per_component_control 1 --component_id 0 --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action SetTotalPower --domain_id 0 --value 100 --
per_component_control 1 --component_id 0 --remote_saa /root/saa
```

```
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.

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 are the supported options for the --action DelTotalPower 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. 0 - Power budget should be applied to whole domain (persistent setting). 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 PECI 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 PECI 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 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action DelTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID> [--remote_saa <remote SAA path>]

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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action DelTotalPower --domain_id <Domain ID> --per_component_control <Per-component Control> --component_id <Component ID> [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action DelTotalPower --domain_id 0 --
per_component_control 1 --component_id 0 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action DelTotalPower --domain_id 0 --per_component_control 1 --
component_id 0 --remote_saa /root/saa
```

```
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.

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 systemm.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action

	SetPowerDrawRange --domain_id <Domain ID> --range <Range> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range>
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action SetPowerDrawRange --domain_id <Domain ID> --range <Range> [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action SetPowerDrawRange --domain_id 0
--range 0-32767 --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action SetPowerDrawRange --domain_id 0 --range 0-32767 --
remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c GeneralNmManage --type BMC10 --action GetSummary [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GeneralNmManage --type BMC10 --action GetSummary
Remote In-Band	saa -I Remote_INB -l <system list file> -c GeneralNmManage --type BMC10 --action GetSummary [--remote_saa <remote SAA path>]

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 -c GeneralNmManage --type BMC10 --action GetSummary
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c GeneralNmManage --type BMC10 --action GetSummary --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c GeneralNmManage --type
BMC10 --action GetSummary --remote_saa /root/saa
```

```
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.

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

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action GetPState [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetPState
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action GetPState [--remote_saa <remote SAA path>]

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 NmCpuManage --type NM20 --action GetPState
```

The console output contains the following information.

```
Current maximum allowed P-State: 0
Number of P-State: 16
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCpuManage --type NM20 --action GetPState --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 -
-action GetPState --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action GetTState [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetTState
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action GetTState [--remote_saa <remote SAA path>]

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 NmCpuManage --type NM20 --action GetTState
```

The console output contains the following information.

```
Current maximum allowed T-State: 0
Number of T-State: 1
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCpuManage --type NM20 --action GetTState --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 --action GetTState --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action GetPTState [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetPTState
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action GetPTState [--remote_saa <remote SAA path>]

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 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)
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCpuManage --type NM20 --action GetPTState --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 -
-action GetPTState --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action GetCPUCores [--remote_saa <remote SAA path>]

Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetCPUCores
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action GetCPUCores [--remote_saa <remote SAA path>]

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 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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCpuManage --type NM20 --action GetCPUCores --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 -
-action GetCPUCores --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action GetCPUMemTemp [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetCPUMemTemp
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action GetCPUMemTemp [--remote_saa <remote SAA path>]

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 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)
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCpuManage --type NM20 --action GetCPUMemTemp --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 -
-action GetCPUMemTemp --remote_saa /root/saa
```

```
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.

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 GetHostCPUData
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action GetHostCPUData [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action GetHostCPUData
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action GetHostCPUData [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCpuManage --type NM20 --action GetHostCPUData
```

In-Band:

```
[SAA_HOME]# ./saa -c NmCpuManage --type NM20 --action GetHostCPUData
```

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCpuManage --type NM20 --action GetHostCPUData --remote_saa /root/saa
```

Multiple OOB:

```
[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c NmCpuManage --type
NM20 --action GetHostCPUData
```

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

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 -
-action GetHostCPUData --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value <assignment value> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value <assignment value>
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action SetMaxAllowedPState --value <assignment value> [--remote_saa <remote SAA path>]

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 NmCpuManage --type NM20 --action SetMaxAllowedPState --value 0
```

The console output contains the following information.

```
NmCpuManage command is completed.
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCpuManage --type NM20 --action SetMaxAllowedPState --value 0 --
remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 -
-action SetMaxAllowedPState --value 0 --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value <assignment value> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value <assignment value>
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value <assignment value> [--remote_saa <remote SAA path>]

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 NmCpuManage --type NM20 --action SetMaxAllowedTState --value 0
```

The console output contains the following information.

```
NmCpuManage command is completed.
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCpuManage --type NM20 --action SetMaxAllowedTState --value 0 --
```

```
remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 -
-action SetMaxAllowedTState --value 0 --remote_saa /root/saa
```

```
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.

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 logical cores. 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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value <assignment value> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value <assignment value>
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value <assignment value> [--remote_saa <remote SAA path>]

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 NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value 0
```

The console output contains the following information.

```
NmCpuManage command is completed.
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCpuManage --type NM20 --action SetMaxAllowedCPUCores --value 0 --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM20 -
-action SetMaxAllowedCPUCores --value 0 --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM40 --action GetTurboSyncRatio --socket <Socket number> --core <Core number> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM40 --action GetTurboSyncRatio --socket <Socket number> --core <Core number>
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM40 --action GetTurboSyncRatio --socket <Socket number> --core <Core number> [--remote_saa <remote SAA path>]

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 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]
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCpuManage --type NM40 --action GetTurboSyncRatio --socket 0 --core
255 --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM40 -
-action GetTurboSyncRatio --socket 0 --core 255 --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket <Socket number> --limit <limit> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket <Socket number> --limit <limit>
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket <Socket number> --limit <limit> [--remote_saa <remote SAA path>]

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 NmCpuManage --type NM40 --action SetTurboSyncRatio --socket 0 --limit 0
```

The console output contains the following information.

```
Done
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCpuManage --type NM40 --action SetTurboSyncRatio --socket 0 --limit
0 --remote_saa /root/saa
```

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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCpuManage --type NM40 -
-action SetTurboSyncRatio --socket 0 --limit 0 --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action GetCUPSCapability [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSCapability
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action GetCUPSCapability [--remote_saa <remote SAA path>]

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 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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCupsManage --type NM30 --action GetCUPSCapability --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30 --action GetCUPSCapability --remote_saa /root/saa
```

```
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.

5.17.4.2 Getting the CUPS Data

Use the NmCupsManage command with option --action GetCUPSData 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 GetCUPSData
In-Band	saa -c NmCupsManage --type NM30 --action GetCUPSData
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action GetCUPSData [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSData
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action GetCUPSData [--remote_saa <remote SAA path>]

Example:

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c NmCupsManage --type NM30 --action GetCUPSData
```

In-Band:

```
[SAA_HOME]# ./saa -c NmCupsManage --type NM30 --action GetCUPSData
```

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)
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCupsManage --type NM30 --action GetCUPSData --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30
--action GetCUPSData --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action GetCUPSConfig [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSConfig
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action GetCUPSConfig [--remote_saa <remote SAA path>]

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 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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCupsManage --type NM30 --action GetCUPSConfig --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30
--action GetCUPSConfig --remote_saa /root/saa
```

```
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.

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.

Single System	
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

Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action GetCUPSPolicy [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSPolicy
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action GetCUPSPolicy [--remote_saa <remote SAA path>]

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 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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCupsManage --type NM30 --action GetCUPSPolicy --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30
--action GetCUPSPolicy --remote_saa /root/saa
```

```
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.

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.

Single System	
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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action GetCUPSCore [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSCore
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action GetCUPSCore [--remote_saa <remote SAA path>]

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 NmCupsManage --type NM30 --action GetCUPSCore
```

The console output contains the following information.

```
Core CUPS = 0
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCupsManage --type NM30 --action GetCUPSCore --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30
--action GetCUPSCore --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action GetCUPSIO [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSIO
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action GetCUPSIO [--remote_saa <remote SAA path>]

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 NmCupsManage --type NM30 --action GetCUPSIO
```

The console output contains the following information.

```
IO CUPS = 0
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCupsManage --type NM30 --action GetCUPSIO --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30
--action GetCUPSIO --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action GetCUPSMem [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action GetCUPSMem
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action GetCUPSMem [--remote_saa <remote SAA path>]

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 NmCupsManage --type NM30 --action GetCUPSMem
```

The console output contains the following information.

```
Memory CUPS = 0
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCupsManage --type NM30 --action GetCUPSMem --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30 --action GetCUPSMem --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action

	SetCUPSPolicy --domain_id <Domain ID> --storage <Storage> --alert <Alert> --threshold <Threshold> --avg_window <averaging window> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < 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>
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action SetCUPSPolicy --domain_id <Domain ID> --storage <Storage> --alert <Alert> --threshold <Threshold> --avg_window <averaging window> [--remote_saa <remote SAA path>]

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 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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c NmCupsManage --type NM30 --action SetCUPSPolicy --domain_id 1 --
```

```
storage 1 --alert 1 --threshold 50 --avg_window 2000 --remote_saa
/root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30
--action SetCUPSPolicy --domain_id 1 --storage 1 --alert 1 --threshold 50
--avg_window 2000 --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action EnableCUPSPolicy --domain_id <Domain ID> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action EnableCUPSPolicy --domain_id <Domain ID>
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action EnableCUPSPolicy --domain_id <Domain ID> [--remote_saa <remote SAA path>]

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 NmCupsManage --type NM30 --action EnableCUPSPolicy --domain_id 1
```

The console output contains the following information.

```
Done.
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCupsManage --type NM30 --action EnableCUPSPolicy --domain_id 1 --
remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30
--action EnableCUPSPolicy --domain_id 1 --remote_saa /root/saa
```

```
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.

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>
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c NmCupsManage --type NM30 --action DisableCUPSPolicy --domain_id <Domain ID> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c NmCupsManage --type NM30 --action DisableCUPSPolicy --domain_id <Domain ID>
Remote In-Band	saa -I Remote_INB -l <system list file> -c NmCupsManage --type NM30 --action DisableCUPSPolicy --domain_id <Domain ID> [--remote_saa <remote SAA path>]

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 NmCupsManage --type NM30 --action DisableCUPSPolicy --domain_id 1
```

The console output contains the following information.

```
Done.
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c NmCupsManage --type NM30 --action DisableCUPSPolicy --domain_id 1 --
remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c NmCupsManage --type NM30
--action DisableCUPSPolicy --domain_id 1 --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c BmcNmManage --type BMC10 --action GetDeviceID [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcNmManage --type BMC10 --action GetDeviceID
Remote In-Band	saa -I Remote_INB -l <system list file> -c BmcNmManage --type BMC10 --action GetDeviceID [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111
-c BmcNmManage --type BMC10 --action GetDeviceID --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c BmcNmManage --type BMC10
--action GetDeviceID --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c BmcNmManage --type BMC10 --action GetPower [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcNmManage --type BMC10 --action GetPower
Remote In-Band	saa -I Remote_INB -l <system list file> -c BmcNmManage --type BMC10 --action GetPower [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c BmcNmManage --type BMC10 --action GetPower --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c BmcNmManage --type BMC10
--action GetPower --remote_saa /root/saa
```

```
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.

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
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c BmcNmManage --type BMC10 --action GetTemp [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcNmManage --type BMC10 --action GetTemp

Remote In-Band	saa -I Remote_INB -l <system list file> -c BmcNmManage --type BMC10 --action GetTemp [--remote_saa <remote SAA path>]

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)
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.56 --ou root --op 111111 -c BmcNmManage --type BMC10 --action GetTemp --remote_saa /root/saa
```

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
```

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c BmcNmManage --type BMC10 --action GetTemp --remote_saa /root/saa
```

```
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.

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 (**Legacy**)	**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]
Remote In-Band	saa -I Remote_INB -u <username> -p <password>} --oi <OS IP address> --ou <OS username> --op <OS password> -c GetTpmInfo [--showall] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetTpmInfo [--showall]
Remote In-Band	saa -I Remote_INB -l <system list file> -c GetTpmInfo [--showall] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c GetTpmInfo --showall
```

```
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 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: 0x50000001
        ReadSizeOfSelect: 0x0003
        ReadPCRSelect[0]: 0x00
        ReadPCRSelect[1]: 0x00
        ReadPCRSelect[2]: 0x00
        ReadLocalityAtRelease: 0x1F
        ReadDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
        WriteSizeOfSelect: 0x0003
        WritePCRSelect[0]: 0x00
        WritePCRSelect[1]: 0x00
        WritePCRSelect[2]: 0x00
        WriteLocalityAtRelease: 0x1F
        WriteDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
        Tag1: 0x0017
        Attributes: 0x00002000
        bReadSTClear: 0x00
        bWriteSTClear: 0x00
        bWriteSDefine: 0x01
        LCP Policy:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 20 32 63
        66 33 65 39 E1 00 00 00 00 00 00 10 0E 39 02
        00 00 00 00 88 78

TPM 1.2 AUX NV index LCP Definition
===================================
    [NV Public Data]
        Tag: 0x0018
        NV index: 0x50000003
        ReadSizeOfSelect: 0x0003
        ReadPCRSelect[0]: 0x00
```

```
        ReadPCRSelect[1]: 0x00
        ReadPCRSelect[2]: 0x00
        ReadLocalityAtRelease: 0x1F
        ReadDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
        WriteSizeOfSelect: 0x0003
        WritePCRSelect[0]: 0x00
        WritePCRSelect[1]: 0x00
        WritePCRSelect[2]: 0x00
        WriteLocalityAtRelease: 0x18
        WriteDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
        Tag1: 0x0017
        Attributes: 0x00000000
        bReadSTClear: 0x00
        bWriteSTClear: 0x00
        bWriteSDefine: 0x00
        LCP Policy:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

TPM 1.2 PPI NV index LCP Definition
===================================
    [NV Public Data]
        Tag: 0x0018
        NV index: 0x50010000
        ReadSizeOfSelect: 0x0003
        ReadPCRSelect[0]: 0x00
        ReadPCRSelect[1]: 0x00
        ReadPCRSelect[2]: 0x00
        ReadLocalityAtRelease: 0x1F
        ReadDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
        WriteSizeOfSelect: 0x0003
        WritePCRSelect[0]: 0x00
        WritePCRSelect[1]: 0x00
        WritePCRSelect[2]: 0x00
        WriteLocalityAtRelease: 0x1F
        WriteDigestAtRelease:
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
        Tag1: 0x0017
        Attributes: 0x00000001
        bReadSTClear: 0x00
        bWriteSTClear: 0x00
        bWriteSDefine: 0x00
```

```
        LCP Policy:
        00 00 00 00 00 00 00 00 00 00

TPM 1.2 Capability Flags
========================
    [Volatile Flags]
        deactivated: 0
        disableForceClear: 0
        physicalPresence: 0
        physicalPresenceLock: 1
        bGlobalLock: 0
    [Permanent Flags]
        disable: 0
        ownership: 1
        deactivated: 0
        readPubEK: 1
        disableOwnerClear: 0
        allowMaintenance: 0
        physicalPresenceLifetimeLock: 0
        physicalPresenceHWEnable: 0
        physicalPresenceCMDEnable: 1
        FIPS: 0
        enableRevokeEK: 0
        nvLocked: 1
        tpmEstablished: 0
```

The console output contains the following information when installing the TPM 2.0 module.

```
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 GetTpmInfo is executed with option “--showall”. Only Supermicro OTA solution supports option “--showall”.

```
TPM 2.0 PS NV index LCP Definition
==========================
    [NV Public Data]
        NvIndex: 0x01C10103
        NameAlg: SHA256
        Attributes: 0x62040408
        PPWrite: 0
        OWNERWrite: 0
        AuthWrite: 0
        PolicyWrite: 1
        Counter: 0
        Bits: 0
        Extend: 0
        PolicyDelete: 1
        WriteLocked: 0
        WriteAll: 0
        WriteDefine: 0
        WriteStClear: 0
        GlobalLock: 0
        PPRead: 0
        OwnerRead: 0
        AuthRead: 1
        PolicyRead: 0
        NoDA: 1
        Orderly: 0
        ClearStClear: 0
        ReadLocked: 0
        Written: 1
        PolicyRead: 0
        PlatformCreate: 1
        ReadStClear: 0
        AuthPolicy Digest:
        C0 01 C8 00 02 10 D0 FA A4 F4 F4 F8 A7 8E F4 F8
        26 4E 6F 85 55 34 0D 2F 04 18 0F 8C F1 10 FF DD
        Name:
        00 0B 40 7B A7 8D 90 B7 CF 3A A5 3C 0B 83 6D AE
        A7 2A E6 B5 67 15 32 BD 4E EF E4 04 E3 7E A4 EB
        B0 19
        LCP Policy:
        00 03 0B 00 01 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 02 00 00 00 00 00 C8 00 08 30
        00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00

TPM 2.0 AUX NV index LCP Definition
===========================
```

```
    [NV Public Data]
        NvIndex: 0x01C10102
        NameAlg: SHA256
        Attributes: 0x62044408
        PPWrite: 0
        OWNERWrite: 0
        AuthWrite: 0
        PolicyWrite: 1
        Counter: 0
        Bits: 0
        Extend: 0
        PolicyDelete: 1
        WriteLocked: 0
        WriteAll: 0
        WriteDefine: 0
        WriteStClear: 1
        GlobalLock: 0
        PPRead: 0
        OwnerRead: 0
        AuthRead: 1
        PolicyRead: 0
        NoDA: 1
        Orderly: 0
        ClearStClear: 0
        ReadLocked: 0
        Written: 1
        PolicyRead: 0
        PlatformCreate: 1
        ReadStClear: 0
        AuthPolicy Digest:
        EF 9A 26 FC 22 D1 AE 8C EC FF 59 E9 48 1A C1 EC
        53 3D BE 22 8B EC 6D 17 93 0F 4C B2 CC 5B 97 24
        Name:
        00 0B 87 7A 0A B0 02 23 4B C3 A3 61 5C 81 9A BF
        20 C3 0A 5F 2A F9 3F B6 DC 13 F3 B9 B0 59 90 F4
        5A FB
        LCP Policy:
        00 00 00 00 11 09 17 20 07 B0 00 00 00 02 00 00
        00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00
        CA D5 6B 67 FD 9A 84 36 B6 69 0B 50 8F 34 95 94
        95 AD 11 69 8A 2D 9A DE 0F 3D F5 DF A3 6A 0A 5C
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00

TPM 2.0 SGX NV index LCP Definition
============================
    [NV Public Data]
        NvIndex: 0x01C10104
        NameAlg: SHA256
        Attributes: 0x62040404
        PPWrite: 0
        OWNERWrite: 0
```

```
        AuthWrite: 1
        PolicyWrite: 0
        Counter: 0
        Bits: 0
        Extend: 0
        PolicyDelete: 1
        WriteLocked: 0
        WriteAll: 0
        WriteDefine: 0
        WriteStClear: 0
        GlobalLock: 0
        PPRead: 0
        OwnerRead: 0
        AuthRead: 1
        PolicyRead: 0
        NoDA: 1
        Orderly: 0
        ClearStClear: 0
        ReadLocked: 0
        Written: 1
        PolicyRead: 0
        PlatformCreate: 1
        ReadStClear: 0
        AuthPolicy Digest:
        B7 5C E1 94 6F 78 DF 8B AA 42 69 18 DB 09 31 80
        17 E6 B3 8D 04 8C 95 4E 05 C2 C4 F3 4B D4 40 60
        Name:
        00 0B 3E CE D2 44 B7 B3 E8 33 3D A2 A8 C5 5E 9A
        40 22 02 E1 C4 45 E8 D3 5D EE 0F C5 EE 17 8A 05
        54 53
        LCP Policy:
        01 00 00 00 00 00 00 00

TPM 2.0 PPI NV index LCP Definition
============================
    [NV Public Data]
        NvIndex: 0x01C10105
        NameAlg: SHA256
        Attributes: 0x42040409
        PPWrite: 1
        OWNERWrite: 0
        AuthWrite: 0
        PolicyWrite: 1
        Counter: 0
        Bits: 0
        Extend: 0
        PolicyDelete: 1
        WriteLocked: 0
        WriteAll: 0
        WriteDefine: 0
        WriteStClear: 0
        GlobalLock: 0
        PPRead: 0
```

```
        OwnerRead: 0
        AuthRead: 1
        PolicyRead: 0
        NoDA: 1
        Orderly: 0
        ClearStClear: 0
        ReadLocked: 0
        Written: 0
        PolicyRead: 0
        PlatformCreate: 1
        ReadStClear: 0
        AuthPolicy Digest:
        B7 5C E1 94 6F 78 DF 8B AA 42 69 18 DB 09 31 80
        17 E6 B3 8D 04 8C 95 4E 05 C2 C4 F3 4B D4 40 60
        Name:
        00 0B 5B 53 B9 80 E7 36 D4 C3 3B 85 A6 A2 BB 7A
        A5 F6 D3 10 1C EB D3 17 7D 69 8E D1 84 51 02 E2
        D0 1B

TPM 2.0 PO NV index LCP Definition
==========================
    [NV Public Data]
        NvIndex: 0x01C10106
        NameAlg: SHA256
        Attributes: 0x2204000A
        PPWrite: 0
        OWNERWrite: 1
        AuthWrite: 0
        PolicyWrite: 1
        Counter: 0
        Bits: 0
        Extend: 0
        PolicyDelete: 0
        WriteLocked: 0
        WriteAll: 0
        WriteDefine: 0
        WriteStClear: 0
        GlobalLock: 0
        PPRead: 0
        OwnerRead: 0
        AuthRead: 1
        PolicyRead: 0
        NoDA: 1
        Orderly: 0
        ClearStClear: 0
        ReadLocked: 0
        Written: 1
        PolicyRead: 0
        PlatformCreate: 0
        ReadStClear: 0
        AuthPolicy Digest:
        22 03 0B 7E 0B B1 F9 D5 06 57 57 1E E2 F7 FC E1
        EB 91 99 0C 8B 8A E9 77 FC B3 F1 58 B0 3E BA 96
```

```
Name:
00 0B 8D D1 B6 DE A2 9D 5B 82 D7 1B 04 84 83 D6
A9 BF DE B1 A9 34 46 AA 96 09 FF D6 AF BE BC 95
7C 19
LCP Policy:
00 03 0B 00 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 02 00 00 00 00 00 C8 00 08 30
00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00
```



Notes:

- This command is supported on X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets or later platforms.
- The field “TPM Locked” in “TPM Information” section is only for TPM 1.2.
- The “Capability Flags” section is only for TPM 1.2.
- The --showall option is optional for the GetTpmInfo command.
- The “PS NV INDEX LCP Definition,” “AUX NV INDEX LCP Definition,” “PPI NV INDEX LCP Definition” ,and “Capability Flags” sections will 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...]
Remote In-Band	saa -I Remote_INB -u <username> -p <password>} --oi <OS IP address> --ou <OS username> --op <OS password> -c TpmManage --

	provision [options...] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c TpmManage [options...]
Remote In-Band	saa -I Remote_INB -l <system list file> -c TpmManage [options...] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111 -c TpmManage --provision --table_default --reboot
```

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

Multiple Systems Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c TpmManage --provision --
table_default --reboot
```

```
[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c TpmManage --provision --
table Tpm12Prov.bin --reboot
```

```
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 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 smbid --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 smbid --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 smbid --pw_file smbpasswd.txt --reboot --lock yes
```

```
smbpasswd.txt
smbpasswd
```



Notes:

- The TpmProvision command is supported from the X10 Intel® Xeon® Processor E5 v3/v4 Product Family to the X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets platforms.
- The TPM ISO images are not included in the 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]
Remote In-Band	saa -I Remote_INB -u <username> -p <password>} --oi <OS IP address> --ou <OS username> --op <OS password> -c TpmManage {options…} [--reboot] [--remote_saa <remote SAA path>]
Multiple Systems	
Multiple Systems	saa -l <system list file> [-u <username> -p <password>] -c TpmManage {options…} [--reboot]
Remote In-Band	saa -I Remote_INB -l <system list file> -c TpmManage {options…} [--reboot] [--remote_saa <remote SAA path>]

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
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c TpmManage --clear_and_enable_dtpm_txt --reboot
```

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c TpmManage --clear_dtpm --reboot

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c TpmManage --enable_txt_and_dtpm --reboot

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c TpmManage --clear_and_enable_dtpm --reboot

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c TpmManage --disable_dtpm --reboot

[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c TpmManage --disable_txt --reboot
```

Multiple OOB:

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

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TpmManage --
clear_dtpm --reboot

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TpmManage --
enable_txt_and_dtpm --reboot

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TpmManage --
clear_and_enable_dtpm --reboot

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c TpmManage --
disable_dtpm --reboot

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

```
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 TpmManage --
clear_and_enable_dtpm_txt --reboot

[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c TpmManage --clear_dtpm --
reboot

[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c TpmManage --
enable_txt_and_dtpm --reboot

[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c TpmManage --
clear_and_enable_dtpm --reboot

[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c TpmManage --disable_dtpm
--reboot

[SAA_HOME]# ./saa -I Remote_INB -l Slist.txt -c TpmManage --disable_txt -
-reboot
```

```
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.



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 smbid --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 smbid --pw smbpasswd --cleartpm --reboot
```



Note:

The TpmProvision command is supported from the X10 Intel® Xeon® Processor E5 v3/v4 Product Family to the X11 Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets platform.

5.18.2. 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 [--post_complete]]

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] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BiosRotManage --action <action> [--redfish] [--file <evidence.bin.gz> [--overwrite]] [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c BiosRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]] [--reboot] [--remote_saa <remote SAA path>]

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	saa -i <IP or host name> -u <username> -p <password> -c BmcRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c BmcRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]]
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 BmcRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c BmcRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c BmcRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]]

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>

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 CpldRotManage --action <action>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c CpldRotManage --action <action>
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -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.
```

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 CpldRotManage --action UpdateGolden
```

Multiple Systems OOB:

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

5.18.5. 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 manage system as the default nonce. When the managed system generates measurement files, the nonce will be written into the files. Thus, whenever a measurement file generates, the digital signature should not be reproduced if the managed system states was not changed.
- **Listing the Existing Measurement Files**
  Use the "--action List" option to list existing measurement files on the managed system.
- **Downloading Existing Measurement Files**
  Use the "--action Download" option to download an existing measurement file on the managed system.
  - Use the --file option to specify the measurement file on managed system.
- **Deleting Existing Measurement Files**
  Use the "--action Delete" option to delete an existing measurement file on the managed system.
  - Use the --file option to specify the measurement file on managed system.
- **Getting Information from Local Measurement Files**
  Use the "--action GetInfo" option to get information from local measurement files.
  - The GetInfo is only available for in-band usage and requires the --file and --file_only option.

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

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

  Use the “--action Compare” option to compare managed system status or local measurement file with a referenced measurement file.
  - The action Compare requires --ref option, use the --ref option to specify the local referenced measurement file, the action Compare will dump a latest measurement from managed system and compare it with the local referenced measurement file.
  - Use the --file option to specify a local measurement file, the action Compare will compare the local measurement file with the local referenced measurement file, to check the local measurement and the referenced measurement are not both tampered, action Compare will still dump a latest measurement from managed system and check the certificate chain and signature states for the measurement files.
  - The --nonce option is also available with the Compare action; the nonce will be written into the latest measurement from managed system. Without the --nonce input, SAA will use the current OS time of the manage 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 -l <system list file> [-u <username> -p <password>] -c Attestation --action <action> [--file <filename> [--overwrite]]
Remote In-Band	saa -I Remote_RHI -l <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:
A30CFFC59284658300654B8CDD5144B7C8CCDF3540B52EAF98FE0B7A3A8A4BB1E7FEA2D89FC9F7BB7
01B35C1DDD53B43E08751F483573DB75E9F3D5653B0871A
```

```
[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 -I 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	saa -i <IP or host name> -u <username> -p <password> -c SetLockdownMode {--lock <yes | no>} [--reboot [--post_complete]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c SetLockdownMode {--lock <yes | no>} [--reboot [--post_complete]]

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.

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

- **Deleting all keys**
  Use the “SecureBootManage” command with the “--action DeleteAllKeys” option to delete all 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.

- The default BIOS setting for secure boot mode is Custom, and there is no secure boot key. The default setting does not enable secure boot. Before enabling secure boot, either add the key, or change the secure boot mode to Standard using the ChangeBiosCfg command.

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 --action <action> [--file_type <file type> [--file <CertificateFile>]] [--reboot [--post_complete]]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c SecureBootManage --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 --action <action> [--file_type <file type> [--file <CertificateFile>]] [--reboot] [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SecureBootManag --action <action> [--file_type <file type> [--file <CertificateFile>]] [--individually]] [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c SecureBootManage --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 --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 --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 --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 --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<br/>
    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.<br/>
```

Multiple Systems OOB:

[SAA_HOME]# ./saa -l Slist.txt -u ADMIN -p PASSWORD -c SecureBootManage --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 --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	1. 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>]] | --precheck 2. saa -i <IP or host name> -u <username> -p <password> -c SecureEraseRaidHdd --tsk_id <task id> [--sync]
In-Band	1. saa -I 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>]] | --precheck 2. saa -I Redfish_HI -u <username> -p <password> -c SecureEraseRaidHdd --tsk_id <task id> [--sync]
Remote In-Band	1. saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c SecureEraseRaidHdd [--dev_id <device_id> [--enc_id <enclosure id>] [--dsk_id <disk id>] [--sync] [--type <BRCM_IT|BRCM_IR>]] | --precheck 2. saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c SecureEraseRaidHdd --tsk_id <task id> [--sync]
Multiple Systems	
OOB	1. saa -I < 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>]] | --precheck

	2. saa -l < system list file > [-u <username> -p <password>] -c SecureEraseRaidHdd --tsk_id <task id> [--sync]
Remote In-Band	1. saa -l Remote_RHI -l <system list file> -c SecureEraseRaidHdd [--dev_id <device_id> [--enc_id <enclosure id>] [--dsk_id <disk id>] [--sync] [--type <BRCM_IT|BRCM_IR>]] | --precheck 2. saa -l Remote_RHI -l <system list file> -c SecureEraseRaidHdd --tsk_id <task id> [--sync]

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.

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

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
```

In-Band:

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

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_RHI --oi 192.168.34.57 --ou root --op 111111 -u ADMIN -p ADMIN -c SecureEraseRaidHdd --dev_id 0 --enc_id 0,1,2 --dsk_id 0,1,2 --remote_saa /root/saa
```

Multiple Systems OOB:

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

```
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 SecureEraseRaidHdd --precheck --remote_saa /root/saa
```

```
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 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 -I 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 OOB:

```
[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[1]	Broadcom SAS 3808
AOC-S3816L-L16iT1[1]	Broadcom SAS 3816
AOC-SLG4-2H8M2[1]	Broadcom SAS 3808
AOC-SMG4-2M2	Broadcom SAS 3808N
AOC-SMG4-2E1S	Broadcom SAS 3808N
AOM-S3808NI-4NM	Broadcom SAS 3808N
AOM-M3808NI-4HM	Broadcom SAS 3808N
AOC-S4116L-H16iR(-16DD/-96DD)	Broadcom SAS 4116

If the target disk is accepted for secure erase or it is being securely erased, there will be a task ID. If the target disk is not allowed for secure erase, there is no task ID. Please remember the task ID(s) for futher polling status purpose.

You can also poll the erasing status right after issuing the command by appending --sync option after the command “SecureEraseRaidHdd”.

Example:

```
[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...
```

3. 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 -I 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:

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 |     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 OOB:

```
[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 -I 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:

OOB:

```
[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 OOB:

```
[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	HR1MJDCKLH4CD88ELEGDUE5J4UA3QGZZ	123456	111111

PSID.txt

```
W472TJXH; HR1MJDCKLH4CD88ELEGDUE5J4UA3QGZZ
```

Password.txt

```
9XF4AF7M; 123456; 111111
W472TJXH; 123456; 111111
```

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c SecureEraseDisk [--current_password <current password> | --cur_pw_file <current password file path>] --file <filename> --precheck [--json_view] saa -i <IP or host name> -u <username> -p <password> -c SecureEraseDisk [--current_password <current password> | --cur_pw_file <current password file path>] --file <filename> --action <action> [--reboot [--post_complete]]
In-Band	saa -c SecureEraseDisk [--current_password <current password> | --cur_pw_file <current password file path>] --file <filename> --precheck [--json_view] saa -c SecureEraseDisk [--current_password <current password> | --cur_pw_file <current password file path>] --file <filename> --action <action> [--reboot]
Remote In-Band	saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SecureEraseDisk [--current_password <current password> | --cur_pw_file <current password file path>] --file <filename> --precheck [--json_view] saa -I Remote_INB --oi <OS IP address> --ou <OS username> --op <OS password> -c SecureEraseDisk [--current_password <current password> | --cur_pw_file <current password file path>] --file <filename> --action <action> [--reboot]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c SecureEraseDisk --file <filename> --precheck [--json_view] saa -l <system list file> [-u <username> -p <password>] -c SecureEraseDisk --file <filename> --action <action> [--reboot [--post_complete]]
Remote In-Band	saa -I Remote_INB -l <system list file> -c SecureEraseDisk --file <filename> --precheck [--json_view]

	saa -I Remote_INB -l <system list file> -c SecureEraseDisk --file <filename> --action <action> [--reboot [--post_complete]]

For Multiple Systems usage, the managed systems should be enumerated row by row in the system list file. For the “SecureEraseDisk” command, the system list file format is fixed for specific commands. Please refer to 5.4.3. Getting Current BIOS Settings.

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 Number ..................S45RNE0M600194
    Password Status ................NOT INSTALLED
    Security Mode ..................SAT3 Supported
    Applicable Action...............SetPassword
                    ...............SecurityErase
[HDD]
```

```
    Serial Number.................W472TJXH
    Password Status...............INSTALLED
    Security Mode.................TCG Supported
    TCG Device Type...............TCG-Enterprise
    Applicable Action.............SecurityErasePWD
                      .............SecurityErasePSID
                      .............ChangePassword
                      .............ClearPassword
Estimated security erase time......33 Minutes
Please check PreCheckFile for the mismatched HDDs.
```

Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB --oi 192.168.34.57 --ou root --op 111111
-c SecureEraseDisk --action SetPassword --file Password.txt --reboot
```

Multiple Systems OOB:

```
[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
```

Multiple Remote In-Band:

```
[SAA_HOME]# ./saa -I Remote_INB -l SList.txt -c SecureEraseDisk --action
SecurityErasePWD --file Password.txt --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 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 Number ..................9XF4AF7M
    Password Status ................NOT INSTALLED
    Security Mode ..................SAT3 Supported
    Applicable Action..............SetPassword
                     ..............SecurityErase
[HDD]
    Serial Number..................W472TJXH
    Password Status................NOT INSTALLED
    Security Mode..................TCG Supported
    TCG Device Type................TCG-Enterprise
    Applicable Action..............SetPassword
                     ..............SecurityErase
Estimated security erase time......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.



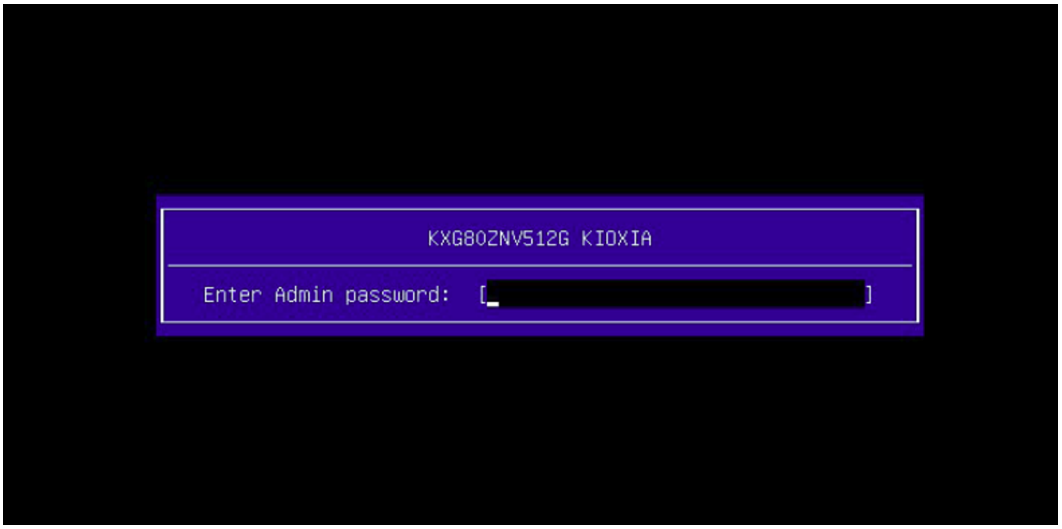
After the task is complete, use the SAA GetCurrentBiosCfg command to check the result through BIOS configurations. Find the status code in the configuration file in xml format by searching for “Last Status Code.” A status code of zero indicates that the previous task was successful. For details on the “GetCurrentBiosCfg” command, see 5.4.3 Getting Current BIOS Settings.

4. For systems that do not support security erase automation, the security erase procedure will be halted by the password prompt during system reboot.

The console output will be as follows.

```
......

Status: The managed system 10.184.24.179 is rebooting.

.........................................
.............................................
................................Done
............
.............................................
.............................................
.............................................
.............................................
.............................................
.............................................
.
Status: Security erase for HDD is being set for 10.184.24.179

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

The password prompt will appear during system reboot.



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 Number ..................9XF4AF7M
    Password Status ................NOT INSTALLED
    Security Mode ..................SAT3 Supported
    Applicable Action..............SetPassword
                     ..............SecurityErase
[HDD]
    Serial Number..................W472TJXH
    Password Status................NOT INSTALLED
    Security Mode..................TCG Supported
    TCG Device Type................TCG-Enterprise
    Applicable Action..............SetPassword
                     ..............SecurityErase

Estimated security erase time......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 -I Redfish_HI -u <username> -p <password> -c GetCpuERoTInfo
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetCpuERoTInfo [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetCpuERoTInfo
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetCpuERoTInfo [--remote_saa <remote SAA path>]

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 -l Redfish_HI -u <username> -p <password> -c UpdateCpuERoT --file <filename>
Remote In-Band	saa -l Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateCpuERoT --file <filename> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c UpdateCpuERoT --file <filename>
Remote In-Band	saa -l Remote_RHI -l <system list file> -c UpdateCpuERoT --file

	<filename> [--remote_saa <remote SAA path>]

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>
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c CpuERotManage --action <action> [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c CpuERotManage --action <action>
Remote In-Band	saa -I Remote_RHI -l <system list file> -c CpuERotManage --action <action> [--remote_saa <remote SAA path>]

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>
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 FpgaRotManage --action <action>
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c FpgaRotManage --action <action>
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -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 -I Redfish_HI -u <username> -p <password> -c GetGpuERoTInfo
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetGpuERoTInfo [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetGpuERoTInfo
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetGpuERoTInfo --file <filename> [--remote_saa <remote SAA path>]

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
```

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 GetGpuERoTInfo
```

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
```

Multiple Systems Remote In-Band through Redfish Host Interface:

```
[SAA_HOME]# ./saa -I Remote_RHI -l SList.txt -c GetGpuERoTInfo
```

```
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.

5.18.16. 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]
Multiple Systems	
OOB	saa -l < 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)................0101070083040000000003
        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
                                       EAE75DCE02DD04993075F4ED9803C3B8
        Measurement(1).................010107008304000000003
        Measurement(2).................020107008304004E564300
        Measurement(3).................03010400830100FF
        Measurement(4).................04013300013000F3B4B4DD0B66A1A529
                                       83177E71C697904458ED0452C6431C26
                                       5BE4FA9529D0A1E9983E864FCC74B665
                                       88E66C5E53BAE9
        Measurement(5).................05013300013000F3B4B4DD0B66A1A529
                                       83177E71C697904458ED0452C6431C26
                                       5BE4FA9529D0A1E9983E864FCC74B665
                                       88E66C5E53BAE9
        Measurement(6).................06013300013000F3B4B4DD0B66A1A529
                                       83177E71C697904458ED0452C6431C26
                                       5BE4FA9529D0A1E9983E864FCC74B665
                                       88E66C5E53BAE9
        Measurement(7).................0701330001300000000000000000000000
                                       0000000000000000000000000000000000
                                       0000000000000000000000000000000000
                                       00000000000000
        Measurement(8).................0801330001300000000000000000000000
                                       0000000000000000000000000000000000
                                       0000000000000000000000000000000000
                                       00000000000000
```

Multiple Systems OOB:

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

```
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 for the managed system.

5.18.17. Managing CMM RoT Functions

The “CmmRotManage” command supports the following features on RoT systems:

- **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	saa -l <system list file> [-u <username> -p <password>] -c CmmRotManage --action <action> [--file <evidence.bin.gz> [--overwrite]]

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
```

5.18.18 GB200 Certificate Management

5.18.18.1. Performing Various Certificate Management Actions

The CertManage command in the SuperServer Automation Assistant (SAA) tool facilitates certificate management for the managed system. It allows users to perform a variety of actions such as retrieving a list of certificates, generating Certificate Signing Requests (CSR), uploading certificates, and deleting specific certificates.

Command Options	Descriptions
--action	**Sets action to**: GetCertList GenerateCSR

	UploadCert DeleteCert

Syntax of CertManage:

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

5.18.18.2. Certificate Management Use Cases

5.18.18.2.1 Example 1: Retrieve Certificate List

OOB:

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

In-Band:

```
[SAA_HOME]# ./saa -c CertManage --action GetCertlist
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.3.0 (2025/01/10) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.
Certificate List:
[
        "/redfish/v1/Managers/BMC_0/Truststore/Certificates/7",
        "/redfish/v1/AccountService/LDAP/Certificates/15",
        "/redfish/v1/Managers/BMC_0/NetworkProtocol/HTTPS/Certificates/1"
]
```

Explanation:

- **Purpose**: This command retrieves a list of all certificates available on the system.
- **Output Details**: The output contains the URLs of certificates categorized by their usage, such as:
  - **HTTPS Certificates**: Used for secure web communication.
  - **LDAP Certificates**: Used for authentication via LDAP services.
  - **Truststore Certificates**: Used for validating external entities.
- **Use Case**: This information is useful for auditing or identifying certificates for management actions like updates or deletions.

5.18.18.2.2 Example 2: Gnerate CSR token and write .csr file

The content of config.json file should be as below for generating CSR token

```
{
    "City": "San Francisco",
    "CertificateCollection": {
        "@odata.id":
"/redfish/v1/Managers/BMC_0/NetworkProtocol/HTTPS/Certificates/1"
    },
    "CommonName": "SMCI",
    "Country": "US",
    "Organization": "SuperMicro",
    "OrganizationalUnit": "Server",
    "State": "SanJose",
    "KeyPairAlgorithm": "EC"
}
```

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CertManage --
action GenerateCSR --cfg_file config.json --file out.csr
```

In-Band:

```
[SAA_HOME]# ./saa -c CertManage --action GenerateCSR --cfg_file
config.json --file out.csr
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.3.0 (2025/01/10) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.

Successfully generated the CSR token and wrote it to the out.csr Certificate to
System.
```

Explanation:

- **Purpose**: This command generates a Certificate Signing Request (CSR) token and writes it to a `.csr` file.
- **Configuration Details**: The content of the `config.json` file includes important certificate information such as:
  - **City**: The city in which the certificate is issued.
  - **Common Name**: The common name for the certificate, e.g., "SMCI".
  - **Organization**: The organization requesting the certificate (e.g., "SuperMicro").
  - **Key Pair Algorithm**: The algorithm used for the key pair (e.g., "EC").
- **Output Details**: After executing the command, the system will generate the CSR token and save it to the specified `.csr` file (e.g., `out.csr`).
- **Use Case**: This command is useful when you need to create a new CSR to request a certificate from a Certificate Authority (CA) for secure communications, such as HTTPS.

5.18.18.2.3 Example 3: Uploading the certificate with specific type

The system accepts certificates in PEM format for uploading or replacing. You can use OpenSSL to generate the PEM file from the CSR (Certificate Signing Request) created in Example 2.

Generating a private key:

If a private key is not available, it can be generated using the following command:

```
openssl genrsa -out private.key 2048
```

This command creates a 2048-bit private key and saves it as private.key.:

Generating a Certificate:

To generate the certificate using the CSR from Example 2, run::

```
openssl x509 -req -days 365 -in request.csr -signkey private.key -out
certificate.crt
```

Creating the PEM File:

Once the private key and certificate are generated, combine them into a PEM file using::

```
cat private.key certificate.crt > certificate.pem
```

This combines the private key and certificate into a single certificate.pem file, which can now be uploaded to the system.

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CertManage --
action UploadCert --type LDAP --file certificate.pem
```

In-Band:

```
[SAA_HOME]# ./saa -c CertManage --action UploadCert --type LDAP --file
certificate.pem
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.3.0 (2025/01/10) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.


Successfully uploaded the LDAP Certificate to System.
```

Explanation:

- **Purpose**: This command uploads a certificate to the system for a specific type (e.g., LDAP).
- **Output Details**: The system successfully uploads the specified certificate file (e.g., `certificate.pem`) for the specified type (e.g., LDAP).
- **Use Case**: This command is useful when you need to upload a new certificate to the system for authentication or secure communication purposes, such as for LDAP-based authentication.

5.18.18.2.4 Example 4: Deleting the Certificate with specific type and certificate Id

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c CertManage --
action DeleteCert --type LDAP --certid 14
```

In-Band:

```
[SAA_HOME]# ./saa -c CertManage --action DeleteCert --type LDAP --certid
14
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.3.0 (2025/01/09) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.

Successfully deleted the certificate of type LDAP with ID 14 from the system.
```

Explanation:

- **Purpose**: This command deletes a specific certificate from the system using its type and certificate ID.
- **Output Details**: The system confirms the successful deletion of the specified certificate (e.g., certificate ID `14`) for the specified type (e.g., LDAP).
- **Use Case**: This command is used when you need to remove a certificate from the system, typically to revoke or replace an outdated certificate, or when the certificate is no longer needed.

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>] [--json_view]
In-Band	saa -I Redfish_HI -u <username> -p <password> -c GetMotherboardFpgaInfo [--file <filename>] [--json_view]
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 GetMotherboardFpgaInfo [--file <filename>] [--json_view]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetMotherboardFpgaInfo [--file <filename>] [--json_view]
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -c GetMotherboardFpgaInfo [--file <filename>] [--json_view]

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
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 UpdateMotherboardFpga --file <filename> --reboot
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMotherboardFpga --file <filename> --reboot
Remote In-Band	saa -I Remote_RHI -l <system list file> [--remote_saa <remote SAA path>] -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
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c GetMotherboardMcuInfo [--remote_saa <remote SAA path>]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c GetMotherboardMcuInfo
Remote In-Band	saa -I Remote_RHI -l <system list file> -c GetMotherboardMcuInfo [--remote_saa <remote SAA path>]

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
Remote In-Band	saa -I Remote_RHI -u <username> -p <password> --oi <OS IP address> --ou <OS username> --op <OS password> -c UpdateMotherboardMcu --file <filename> --reboot [--remote_saa <remote SAA path>]
Multiple Systems	

OOB	saa -l < system list file > [-u <username> -p <password>] -c UpdateMotherboardMcu --file <filename> --reboot [--post_complete]
Remote In-Band	saa -I Remote_RHI -l <system list file> -c UpdateMotherboardMcu --file <filename> --reboot [--remote_saa <remote SAA path>]

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.

5.21 Switch Management

5.21.1 Nvidia Switch Management

5.21.1.1 Performing Various Nv Switch Management Actions

The NvSwitchManage command in the SuperServer Automation Assistant (SAA) tool enables firmware and system image management for Nvidia switches. It supports

actions such as retrieving firmware information, updating firmware, checking NVOS (Nvidia OS) status, and updating NVOS system image.

Command Options	Descriptions
--action	**Sets action to**: GetFwInfo UpdateFw GetNvosInfo ShowNvosSysImageList UpdateNvosSysImage

Syntax of NvSwitchManage:

Single System	
OOB	saa -i <IP or host name> -u <username> -p <password> -c NvSwitchManage --action <action>

5.21.1.2 Nv Switch Management Use Cases

5.21.1.2.1 Example 1: Retrieve Component Firmware Info

OOB:

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

The console output contains the following information.

```
SuperServer Automation Assistant 1.4.0 (2025/07/15) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.
Managed system.........................192.168.34.56
    ASIC:
        actual-firmware.................35.2015.1680
        auto-update.....................enabled
        fw-source.......................default
        part-number.....................920-9K36F-00MV-GS0_Ax
```

```
    BIOS:
        actual-firmware.................0ACTV_00.01.012
        fw-source.......................N/A
        part-number.....................N/A
    BMC:
        actual-firmware.................88.0002.0956
        fw-source.......................N/A
        part-number.....................692-13809-1404-000
    CPLD1:
        actual-firmware.................CPLD000370_REV0500
        fw-source.......................N/A
        part-number.....................0x0172
    CPLD2:
        actual-firmware.................CPLD000377_REV0800
        fw-source.......................N/A
        part-number.....................0x0179
    CPLD3:
        actual-firmware.................CPLD000373_REV0800
        fw-source.......................N/A
        part-number.....................0x0175
    CPLD4:
        actual-firmware.................CPLD000390_REV0300
        fw-source.......................N/A
        part-number.....................0x0186
    EROT:
        active..........................flash1
        actual-firmware.................01.04.0008.0000_n04
        ap-boot-status..................0x000201fd00501120
        background-copy-status..........completed
        debug-token-status..............not-installed
        fw-source.......................N/A
        inactive........................flash2
        part-number.....................N/A
    EROT-ASIC1:
        active..........................flash1
        actual-firmware.................01.04.0008.0000_n04
        ap-boot-status..................0x000201fd00501120
        background-copy-status..........completed
        debug-token-status..............not-installed
        fw-source.......................N/A
        inactive........................flash2
        part-number.....................N/A
    EROT-ASIC2:
        active..........................flash1
        actual-firmware.................01.04.0008.0000_n04
        ap-boot-status..................0x000201fd00501120
        background-copy-status..........completed
        debug-token-status..............not-installed
        fw-source.......................N/A
        inactive........................flash2
        part-number.....................N/A
    EROT-BMC:
        active..........................flash1
```

```
        actual-firmware.................01.04.0008.0000_n04
        ap-boot-status..................0x000501fd00401120
        background-copy-status..........completed
        debug-token-status..............not-installed
        fw-source.......................N/A
        inactive........................flash2
        part-number.....................N/A
    EROT-CPU:
        active..........................flash1
        actual-firmware.................01.04.0008.0000_n04
        ap-boot-status..................0x000101fd00401120
        background-copy-status..........pending
        debug-token-status..............not-installed
        fw-source.......................N/A
        inactive........................flash2
        part-number.....................N/A
    EROT-FPGA:
        active..........................flash1
        actual-firmware.................01.04.0008.0000_n04
        ap-boot-status..................0x000601fd00501120
        background-copy-status..........completed
        debug-token-status..............not-installed
        fw-source.......................N/A
        inactive........................flash2
        part-number.....................N/A
    FPGA:
        actual-firmware.................0.1A
        fw-source.......................N/A
        part-number.....................N/A
    SSD:
        actual-firmware.................CE00A400
        fw-source.......................N/A
        part-number.....................Virtium VTPM24CEXI080-BM110006
    transceiver:
        actual-firmware.................N/A
        fw-source.......................N/A
        part-number.....................N/A
```

Explanation:

- **Purpose**:
  This command retrieves the complete firmware inventory from the managed system, including detailed firmware versions and status for components such as ASIC, BIOS, BMC, CPLDs, EROT modules, FPGA, SSD, and transceivers.

- **Output Details**:
  The output provides a hierarchical and categorized view of the system's firmware data:

- **ASIC / BIOS / BMC**: Shows actual firmware versions, part numbers, and firmware source.
- **CPLD1–CPLD4**: Displays CPLD revision levels and part numbers for hardware programmable logic controllers.
- **EROT Modules**: Lists active/inactive partitions, boot status, background copy status, and debug token installation state across various functional domains (ASIC, BMC, CPU, FPGA).
- **FPGA / SSD**: Includes current firmware versions and vendor-specific part numbers.

- **Use Case**:
  This output is essential for users to:

  - Verify current system firmware before performing upgrades.

5.21.1.2.2 Example 2: Retrieve Specific Component Firmware Info

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c nvswitchmanage
--action GetFwInfo --comp BMC
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.4.0 (2025/07/15) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.
Managed system.......................192.168.34.56
        actual-firmware.................88.0002.0956
        fw-source.......................N/A
        part-number.....................692-13809-1404-000
```

Explanation:

- **Purpose**:
  This command retrieves firmware information for a specific component—in this example, the `BMC`—from the managed Nvidia switch system.

- **Output Details**:
  The output includes:

  - **actual-firmware**: The currently active firmware version on the selected component.
  - **fw-source**: Indicates the source of the firmware, such as default, user-provided, or N/A.
  - **part-number**: The hardware part number associated with the firmware, useful for inventory and support purposes.

- **Use Case**:
  Useful when an administrator needs to:

  - Check the firmware version of a specific component without parsing the full inventory.
  - Verify upgrade success or firmware consistency for individual components such as `ASIC`, `BMC`, `BIOS`, `FPGA`, etc.
  - Troubleshoot version-specific firmware issues on targeted modules.

5.21.1.2.3 Example 3: Updating the Specific Nv Switch Component

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c nvswitchmanage
--action updatefw --comp erot --file nvfw_GB200-
P4978_0004_250213.1.0_prod-signed.fwpkg --reboot
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.4.0 (2025/07/15) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.
Managed system.........................192.168.34.56
        active.........................flash1
        actual-firmware................01.04.0008.0000_n04
        ap-boot-status.................0x000201fd00501120
        background-copy-status.........completed
        debug-token-status.............not-installed
        fw-source......................N/A
        inactive.......................flash2
        part-number....................N/A
```

```
Status: Start updating NVOS Component Firmware for 192.168.34.56

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

Uploading component firmware file to NVOS ...
Sending file '/home/saa3/anil/switch_frimwares/nvfw_GB200-
P4978_0004_250213.1.0_prod-signed.fwpkg' to '/host/fw-images/erot/nvfw_GB200-
P4978_0004_250213.1.0_prod-signed.fwpkg' on 192.168.34.56.
.....Done

Updating EROT.............................Done

Rebooting target system.................................................
................................................
................................................
................................................
................................................
................................................
.........................Done

Status: NVOS Component Firmware is updated for 192.168.34.56
```

Explanation:

- **Purpose**:
  This command updates the firmware of a specific component—in this case, `EROT`—on the Nvidia switch using the SuperServer Automation Assistant (SAA). It uploads the specified firmware package and optionally reboots the system to apply changes.

- **Output Details**:
  The output includes multiple stages of the update process:

  - **Component Info**: Shows the current firmware details of the selected component (e.g., active firmware, boot status, background copy status).
  - **Firmware Upload**: Indicates the local file path and the destination path on the target system.
  - **Update Process**: Displays progress and completion status for the firmware update and system reboot.

- **Status Message**: Confirms the firmware update was successful for the specified component and target IP.

- **Use Case**:
  This is useful when:

  - You need to apply a firmware fix or feature enhancement to a specific hardware module like `EROT`, `BMC`, or `ASIC`.
  - You want to perform a targeted firmware update without updating the entire system.
  - You require confirmation of successful update and system reboot in an automated flow.

5.21.1.2.4 Example 4: Retrieve the NVOS Info

OOB:

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

The console output contains the following information.

```
SuperServer Automation Assistant 1.4.0 (2025/07/15) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.
Managed system.........................192.168.34.56
    ImageInfo:
        current.........................nvos-25.02.1885
        next............................nvos-25.02.1885
        partition1......................nvos-25.02.1879
        partition2......................nvos-25.02.1885
    systemDetail:
        build...........................NVOS Debian GNU/Linux 11 (bullseye)
        contact.........................null
        date-time.......................2025-07-15 08:08:13
        health-status...................OK
        hostname........................rack3-nvlsw-slot2
        location........................null
        platform........................x86_64-nvidia_n5110_ld-r0
        product-name....................nvos
        product-release.................25.02.1885
        status..........................System is ready
        swap-memory.....................0 MB used / 0 MB free / 0 MB total
        system-memory...................3991 MB used / 11924 MB free / 15916 MB
total
```

```
        timezone.....................Etc/UTC
        uptime.......................7019
        version:
            build-date................Mon Mar 10 21:15:11 UTC 2025
            image.....................nvos-25.02.1885
            kernel....................5.10.0-30-2-amd64
            onie......................2023.11-5.3.0012-115200
```

Explanation:

- **Purpose**:
  This command retrieves the NVOS (Nvidia OS) runtime and image information from the managed switch system. It provides system-level status including active and staged OS images, system build details, memory usage, and kernel versions.

- **Output Details**:
  The output is divided into two sections:

  - **ImageInfo**: OS image deployment across partitions.

    - `current`: The currently active NVOS image.
    - `next`: The image scheduled for use after reboot.
    - `partition1 / partition2`: The NVOS versions stored in each system partition.

  - **systemDetail**: System identity and health information.

    - `build`, `product-release`, `kernel`: OS version and platform details.
    - `health-status`: System health status (e.g., OK).
    - `hostname`, `uptime`, `timezone`: System environment metadata.
    - `swap-memory` and `system-memory`: Memory consumption details.
    - `version`: Build metadata such as build date, ONIE version, and kernel version.

- **Use Case**:
  Useful for users when need to:

  - Verify current and upcoming NVOS image versions before or after upgrades.

- Monitor system memory and swap usage.
- Check platform readiness and health before rolling out updates.
- Troubleshoot NVOS compatibility and kernel-level issues.

5.21.1.2.5 Example 5: Retrieve the available NVOS image files

OOB:

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

The console output contains the following information.

```
SuperServer Automation Assistant 1.4.0 (2025/07/15) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.
Managed system.........................192.168.34.56
    nvos-amd64-25.02.1638.bin:
        path............................/host/nos-images/nvos-amd64-
25.02.1638.bin
    nvos-amd64-25.02.1686.bin:
        path............................/host/nos-images/nvos-amd64-
25.02.1686.bin
    nvos-amd64-25.02.1782.bin:
        path............................/host/nos-images/nvos-amd64-
25.02.1782.bin
    nvos-amd64-25.02.1877.bin:
        path............................/host/nos-images/nvos-amd64-
25.02.1877.bin
    nvos-amd64-25.02.1879.bin:
        path............................/host/nos-images/nvos-amd64-
25.02.1879.bin
    nvos-amd64-25.02.1885.bin:
        path............................/host/nos-images/nvos-amd64-
25.02.1885.bin
```

Explanation:

- **Purpose**:
  This command lists all NVOS (Nvidia OS) image files currently available on the managed switch system. These images are typically stored on the switch and can be used for system upgrades or rollbacks.

- **Output Details**:
  The output displays:

  - `Image Filename`: Each available NVOS image (e.g., `nvos-amd64-25.02.1885.bin`).
  - `path`: The full path on the system where the image is stored (e.g., `/host/nos-images/`).

  This list helps users confirm which image files are available for deployment or deletion.

- **Use Case**:
  Ideal for scenarios where you need to:

  - Check which NVOS image versions are stored on the system.
  - Verify that the desired image is present before performing an upgrade or downgrade.
  - Audit or clean up unused firmware images from the host storage.

5.21.1.2.6 Example 6: Updating the NVOS System Image

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c nvswitchmanage
--action UpdateNvosSysImage --file nvos-amd64-25.02.2225.bin
```

The console output contains the following information.

```
SuperServer Automation Assistant 1.4.0 (2025/07/15) (x86_64)
Copyright(C) 2024-2025 Super Micro Computer, Inc. All rights reserved.
Managed system.........................192.168.34.56
    ImageInfo:
        current.........................nvos-25.02.1885
        next............................nvos-25.02.1885
        partition1......................nvos-25.02.1879
        partition2......................nvos-25.02.1885
    systemDetail:
        build...........................NVOS Debian GNU/Linux 11 (bullseye)
        contact.........................null
        date-time.......................2025-07-15 05:55:15
        health-status...................OK
```

```
        hostname.....................rack3-nvlsw-slot2
        location.....................null
        platform.....................x86_64-nvidia_n5110_ld-r0
        product-name.................nvos
        product-release..............25.02.1885
        status.......................System is ready
        swap-memory..................0 MB used / 0 MB free / 0 MB total
        system-memory................4408 MB used / 11508 MB free / 15916 MB
total
        timezone.....................Etc/UTC
        uptime.......................256078
        version:
            build-date...............Mon Mar 10 21:15:11 UTC 2025
            image....................nvos-25.02.1885
            kernel...................5.10.0-30-2-amd64
            onie.....................2023.11-5.3.0012-115200

Status: Start updating NVOS System Image for 192.168.34.56

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

Uploading System Image file to NVOS ...
Sending file 'nvos-amd64-25.02.2225.bin' to '/host/nos-images/nvos-amd64-
25.02.2225.bin' on 192.168.34.56.
................................................
................................Done

Updating NVOS system image.....................
................................................
................................................
................................................
..................................... Done

Rebooting target system.............
................................................
................................................
................................................
................................................
................................................ Done

Status: NVOS System Image is updated for 192.168.34.56
```

Explanation:

- **Purpose**:
  This command uploads and activates a new NVOS (Nvidia OS) system image on the managed switch. It updates the OS image stored in the system partitions and reboots the device to apply the changes.

- **Output Details**:
  The output includes:

  - **ImageInfo**: Reflects the current and upcoming NVOS image versions across partitions:

    - `current`: The currently active NVOS image.
    - `next`: The scheduled image to be used after reboot.
    - `partition1` / `partition2`: Stored NVOS image versions in each partition.

  - **systemDetail**: Shows Current overall system metadata:

    - `product-release`, `kernel`, `build-date`: Version and build info.
    - `hostname`, `uptime`, `memory`: System environment and resource usage.
    - `status`: System readiness post-update.

  - **Status Updates**: Real-time logs for upload, image installation, and reboot progress.

- **Use Case**:
  Ideal when users need to:

  - Upgrade to a new NVOS image.



Notes:
- NvSwitchManage command is supported only in GB200 NVL.

5.21.2 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>] [--json_view]
In-Band	saa -c GetBladeSwitchInfo --file <filename> --file_only [--json_view]
Multiple Systems	
OOB	saa -l <system list file> [-u <username> -p <password>] -c GetBladeSwitchInfo [--dev_id <Device ID>] [--file <filename>] [--json_view]

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 OOB:

```
[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.

5.21.3 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	saa -i <Switch IP or switch host name> -u <Switch username> -p <Switch password> -c UpdateBladeSwitch --file <filename> [--reboot] saa -i <CMM IP or CMM host name> -u <CMM username> -p <CMM password> -c UpdateBladeSwitch --file <filename> --dev_id <Switch device ID> --switch_user <Switch username> --switch_pw <Switch password> [--reboot]
Multiple Systems	

OOB	saa -l <system list file> [-u <Switch username> -p <Switch password>] -c UpdateBladeSwitch --file <filename> [--reboot] [--individually] saa -l <system list file> [-u <username> -p <password>] -c UpdateBladeSwitch --file <filename> [--dev_id <Switch device ID> --switch_user <Switch username> --switch_pw <Switch password>] [--reboot] [--individually]

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 --inidividually option usage, if you want to update 192.168.34.100 and 192.168.34.101, you need to provide two files Supermicro_Switch.bin.192.168.34.100 and Supermicro_Switch.bin.192.168.34.101. Then set the --file argument with the “Supermicro_Switch.bin” filename. With the --individually option, 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.

5.21.4 Rebooting the Switch

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



Notes:

- Simultaneously rebooting all switches may cause temporary network disconnection for all blades in the chassis.
- To reboot the managed switch through a CMM IP and a switch device ID, you can use the --dev_id option.
- Please use the GetBladeSwitchInfo command to get the switch device ID.
- To reboot the switch via CMM without switch credentials, use the --dev_id option only.
- To directly reboot the switch with switch IP, please do not use the --dev_id, --switch_user, and --switch_pw options. Please use switch IP and -u and -p (for switch credentials) instead.
- To reboot the switch via CMM with switch credentials, use the --dev_id, --switch_user, and --switch_pw options together.
- Direct reboot via switch IP and credentials is supported only for the following switch modules with the specified minimum firmware versions or above: SBM-25G-P10 (1.0.0.10), MBM-XEM-002 (2.2.1.34), MBM-GEM-004 (1.3.0.8), and SBM-25G-100 (1.4.0.11).

Single System	
OOB	saa -i <Switch IP or switch host name> -u <Switch username> -p <Switch password> -c RebootBladeSwitch saa -i <CMM IP or CMM host name> -u <CMM username> -p <CMM password> -c RebootBladeSwitch --dev_id <Switch device ID>

	saa -i <CMM IP or CMM host name> -u <CMM username> -p <CMM password> -c RebootBladeSwitch --dev_id <Switch device ID> --switch_user <Switch username> --switch_pw <Switch password>
Multiple Systems	
OOB	saa -l <system list file> [-u <Switch username> -p <Switch password>] -c RebootBladeSwitch saa -l <system list file> [-u <username> -p <password>] -c RebootBladeSwitch [--dev_id <Switch device ID>] saa -l <system list file> [-u <username> -p <password>] -c RebootBladeSwitch [--dev_id <Switch device ID> --switch_user <Switch username> --switch_pw <Switch password>]

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

[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

[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
```

5.22 Liquid Cooling Management

5.22.1. Monitoring CDU Status

5.22.1.1. 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>} [--json_view] [--file <CDUStatus.txt> [--overwrite]]
Multiple Systems	
OOB	saa -l < system list file > [-u <username> -p <password>] -c MonitorCDUStatus {--action <GetStatus|1>} [--json_view] [--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
  --------------                 -------
   Top Power Unit 1                Good
```

```
    Bottom Power Unit 2               Good
    Left Pump 1                       Error
    Right Pump 2                      Good
    Left Valve 1                      Good
    Right Valve 2                     Good
    Control Unit                      Good
    Sensor Module                     Good
    CDU Leak Detection                Good
    Humidity Sensor                   Good
    CDU Liquid Level                  Full
    CH1 External Liquid Level         N/A
    CH2 External Liquid Level         N/A
    CH1 External Leak Sensor          N/A
    CH2 External Leak Sensor          N/A
[Sensor Value]
     Sensor Name                       Status               Value
    --------------                    -------              -------
    Coolant Return Temperature         Good                31.30[°C]
    Coolant Supply Temperature         Good                31.25[°C]
    Facility water Supply Temperature  Good                26.38[°C]
    Facility water Return Temperature  Good                27.01[°C]
    Coolant Pressure                   Good                0.018[MPa]
    Facility Pressure                  Good                0.000[MPa]
    Coolant Flow Rate                  Good                50.30[LPM]
    Facility Water Flow Rate           Good                0.00[LPM]
    Ambient Temperature                                    22.51[°C]
    Humidity Sensor                    Good                56.25[RH]
    Dew Point                          Good                13.37[°C]
    Heat Dissipated                                        0.2[kW]
    Rough Power Consumption                                155.95[W]
```

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

5.22.1.2. 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:

OOB:

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

Multiple Systems OOB:

```
[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.

5.22.1.3. CDU Alert Settings JSON File Format

A CDU alert settings JSON file format is explained below. The sample file is named “CDU_alertsetting_sample.json” and bundled in the SAA release package.

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.



Note: MonitorCDUStatus is only supported on liquid-cooling GPU systems with the following CDU models:

- **LCS-SCDU-100L4001** — 100 kW
- **LCS-SCDU-100L4002** — 100 kW
- **LCS-SCDU-100L4003** — 100 kW
- **LCS-SCDU-100L4004** — 100 kW
- **LCS-SCDU-250L4001** — 250 kW
- **LCS-SCDU-250LP4002** — 250 kW

5.22.2. Updating the CDU Firmware Image

Use the "UpdateCDU" command with a CDU firmware bundle image to run SAA to update the CDU firmware of a managed system.

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

OOB:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u ADMIN -p PASSWORD -c UpdateCDU –-
file CDU.zip
```

The console output contains the following information

```
Managed system.................192.168.34.56
    CU Left...................0912
    CU Right..................0912
    Pump Left.................0912
    Pump Right................0912
    Valve Left................0912
    Valve Right...............0912
    Sensor Module.............0911
    Web I/F...................1003
Local CDU image file..........CDU_20231024.zip
    Sensor Version............99.02
    CU/Pump/Valve Version.....99.02
    WebIF Version.............9902
Status: Start updating CDU for 192.168.34.56
**********************************WARNING**************************************
    Do not remove AC power from the server.
*******************************************************************************
Uploading CDU FW..........Done
Updating CDU FW...>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Done
Update Complete.
Device Name: CU Left
        Update Status: Success
Device Name: CU Right
        Update Status: Success
Device Name: Pump Left
        Update Status: Success
Device Name: Pump Right
        Update Status: Success
Device Name: Valve Left
        Update Status: Success
Device Name: Valve Right
        Update Status: Success
Device Name: Sensor module
        Update Status: Success
Device Name: Web I/F
        Update Status: Success
```

Multiple Systems OOB:

[SAA_HOME]# ./saa -l SList.txt -u ADMIN -p PASSWORD -c -c UpdateCDU –-file CDU.zip

```
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.



Note:
UpdateCDU is only supported on liquid-cooling GPU systems with the following CDU models:

- **LCS-SCDU-100L4001** — 100 kW
- **LCS-SCDU-100L4002** — 100 kW
- **LCS-SCDU-100L4003** — 100 kW
- **LCS-SCDU-100L4004** — 100 kW
- **LCS-SCDU-250L4001** — 250 kW
- **LCS-SCDU-250LP4002** — 250 kW

Appendix A. SAA Exit Codes

Exit Code Number	Description
0	Successful
Others	Failed
GROUP1 (1~30) Command line parsing check failed	
1	GetOpt unexpected option code
2	Unknown option
3	Missing argument
4	No host IP/user/password
5	Missing option
6	Unknown command
7	Option conflict
8	Can not open file
9	File already exists
10	Host is unknown
11	Invalid command line data
12	Function access denied
GROUP2 (31~59) Resource management error	
31	File management error
32	Thread management error
33	TCP connection error
34	UDP connection error

35	Program interrupted and terminated
36	Required device does not exist
37	Required device does not work
38	Function is not supported
39	FTP server reports error
40	Http connection error
GROUP3 (60~79) File parsing errors	
60	Invalid configuration file
61	Utility internal error
62	Invalid input file
63	Invalid firmware flash ROM
64	Invalid download file
65	Invalid internal file
GROUP4 (80~90) IPMI operation errors	
80	Node Product key is not activated
81	Internal communication error
82	Board information mismatch
83	Does not support OOB
84	Does not support get file
85	File is not available for download
86	Required tool does not exist
87	IPMI standard error
GROUP5 (91~99) Action Required	

92	Manual reboot is required
GROUP6 (100~119) In-band operation errors	
100	Cannot open driver
101	Driver input/output control failed
102	Driver report: ****execution of command failed****
103	BIOS does not support this in-band command
104	Driver report: ****file size out of range****
105	Cannot load driver
106	Driver is busy. Please try again later
107	ROM chip is occupied. Please try again later
108	Kernel module verification error
109	This operation is prohibited
GROUP7 (120~199) IPMI communication errors	
120	Invalid Redfish response
144	IPMI undefined error
145	IPMI connect failed
146	IPMI login failed
147	IPMI execution parameter validation failed
148	IPMI execution exception occurred
149	IPMI execution failed
150	IPMI execution exception on slave CMM or unavailable
151	IPMI execution exception on module not present

152	IPMI execution only for CMM connected
153	IPMI execution on non-supported device
154	IPMI execution only for BMC connected
155	IPMI delivered invalid data
180	IPMI command not found
181	IPMI command IP format error
182	IPMI command parameter length invalid
GROUP8 (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 Licenses 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	**SFT-OOB-LIC**	
CheckSensorData	**Yes**	No	C	No license required	
ServiceCalls	**Yes**	**Yes**	F + C	**SFT-DCMS-SINGLE + SFT-DCMS-SVC-KEY**	
SystemPFA	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
MemoryHea	**Yes**	**Yes**	C	**SFT-DCMS-**	

lthCheck				**SINGLE**	
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**	
[System Management]					
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	
SetFanMod	**Yes**	**Yes**	C	No license	

e				required	
LocateServerUid	**Yes**	**Yes**	C	No license required	
GetFirmwareInventoryInfo	**Yes**	**Yes**	C	No license required	
ClearCMOS	**Yes**	**Yes**	C	No license required	
[BIOS Management]					
GetBiosInfo	**Yes**	**Yes**	C	No license required	
UpdateBios (without --preserve_setting)	**Yes**	**Yes**	C	No license required	**SFT-OOB-LIC is required for H12 non-RoT systems**
UpdateBios (with --preserve_setting)	**Yes**	**Yes**	C	No license required	**SFT-OOB-LIC is required for:** **• Platforms before (not included) X12 Intel® Xeon® E-2300 Series** **• H12 systems**
GetDefaultBiosCfg	**Yes**	**Yes**	F + C	**SFT-OOB-LIC**	
GetCurrentBiosCfg	**Yes**	**Yes**	F + C	**SFT-OOB-LIC**	
ChangeBiosCfg	**Yes**	**Yes**	F	**SFT-OOB-LIC**	**SFT-DCMS-SINGLE is required for some configuration items**
LoadDefaultBiosCfg	**Yes**	**Yes**	C	**SFT-OOB-LIC**	

SetBiosPassword	**Yes**	**Yes**	F + C	**SFT-OOB-LIC**	
GetDmiInfo	**Yes**	**Yes**	F	**SFT-OOB-LIC**	
ChangeDmiInfo	**Yes**	**Yes**	F	**SFT-OOB-LIC**	
EditDmiInfo	**Yes**	**Yes**	F	**SFT-OOB-LIC**	
EraseOAKey	No	**Yes**	C	No license required	
GetScpInfo	**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	
[BMC Management]					
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	**SFT-OOB-LIC**	
DownloadBmcCfg	**Yes**	**Yes**	F	No license required	
UploadBmcCfg	**Yes**	**Yes**	F	No license required	
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	**SFT-OOB-LIC**	
SetKcsPriv	**Yes**	No	C	**SFT-OOB-LIC**	
LoadDefaultBmcCfg	**Yes**	**Yes**	C	No license required	
GetBmcUserList	**Yes**	**Yes**	C	**No license required**	
SetBmcUserList	**Yes**	**Yes**	C	**No license required**	
BmcReset	**Yes**	**Yes**	C	No license required	
BootStrappingAccount	**Yes**	**Yes**	C	No license required	
RmcpManage	**Yes**	**Yes**	C	**SFT-OOB-LIC**	
GetSessionI	**Yes**	No	C	No license	

nfo				required	
SessionManage	**Yes**	**Yes**	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	
BmcIPv6StaticRouteManage	Yes	**Yes**	C	No license required	
[System Event Log]					
GetEventLog	**Yes**	**Yes**	C	No license required	
ClearEventLog	**Yes**	**Yes**	C	No license required	**SFT-OOB-LIC is required for --clear_bios_eventlog option**
GetMaintenEventLog	**Yes**	**Yes**	C	No license required	
ClearMaintenEventLog	**Yes**	**Yes**	C	No license required	
GetHostDump	**Yes**	**Yes**	F + C	**SFT-DCMS-SINGLE**	
SetSELTimeMode	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
[CMM Management]					

GetCmmInfo	**Yes**	**Yes**	C	No license required	
UpdateCmm	**Yes**	No	C	No license required	
GetCmmCfg	**Yes**	No	F + C	No license required	
ChangeCmmCfg	**Yes**	No	F	No license required	
SetCmmPassword	**Yes**	No	F + C	No license required	
LoadDefaultCmmCfg	**Yes**	No	C	No license required	
GetBbpInfo	**Yes**	No	C	No license required	
UpdateBbp	**Yes**	No	C	No license required	
GetBladePowerStatus	**Yes**	No	C	No license required	
SetBladePowerAction	**Yes**	No	C	No license required	
ProfileManage	**Yes**	No	C	No license required	
BladePsuManage	**Yes**	**Yes**	C	No license required	
BladeSummary	**Yes**	**Yes**	C	No license required	
BladeConsole	**Yes**	No	C	No license required	
GetCmmUserList	**Yes**	**Yes**	C	**SFT-OOB-LIC**	
SetCmmUserList	**Yes**	**Yes**	C	**SFT-OOB-LIC**	
UpdateDum	**Yes**	No	F + C	No license	

mySwitch				required	
BladeNode Manage	**Yes**	**No**	C	No license required	
[Storage Management]					
GetRaidControllerInfo	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
UpdateRaid Controller	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
GetRaidCfg	**Yes**	**Yes**	F + C	**SFT-DCMS-SINGLE**	
ChangeRaid Cfg	**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-SINGLE**	
GetVROCCfg	**Yes**	**Yes**	F + C	**SFT-DCMS-SINGLE**	
ChangeVROCCfg	**Yes**	**Yes**	F	**SFT-DCMS-SINGLE**	
GetSmartData	**Yes**	**Yes**	C	No license required	
GetSasExpanderInfo	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
UpdateSas Expander	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
[PSU Management]					

GetPsuInfo	**Yes**	**Yes**	C	**SFT-OOB-LIC**	
UpdatePsu	**Yes**	**Yes**	F + C	**SFT-DCMS-SINGLE**	
GetPowerStatus	**Yes**	**Yes**	C	No license required	
SetPowerAction	**Yes**	**Yes**	C	No license required	
DcmiManage	**Yes**	**Yes**	C	No license required	
PowerPolicy	**Yes**	**Yes**	C	No license required	
GetAcpiPowerStatus	**Yes**	**Yes**	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	
CpuPowerManage	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
GetPowerShelfInfo	**Yes**	**No**	C	No license required	
UpdatePowerShelf	**Yes**	**No**	C	No license required	
[PCIeSwitch Management]					
GetPCIeSwitchInfo	No	**Yes**	C	No license required	
UpdatePCIeSwitch	No	**Yes**	C	No license required	
[Applications]					

GetUsbAccessMode	No	**Yes**	C	**SFT-DCMS-SINGLE**	
SetUsbAccessMode	No	**Yes**	C	**SFT-DCMS-SINGLE**	
RawCommand	**Yes**	**Yes**	C	No license required	
KmsManage	**Yes**	**Yes**	F + C	**SFT-OOB-LIC**	**SFT-DCMS-SINGLE is required for TLS upload configuration**
RedfishApi	**Yes**	**Yes**	C	No license required	
RemoteExec	No	**Yes (Remote Only)**	F + C	No license required	
RemoteConsole	**Yes**	No	C	No license required	
RemoteScreenshot	**Yes**	**Yes**	F	SFT-DCMS-SINGLE	
RemoteKeyboard	**Yes**	No	F	SFT-DCMS-SINGLE	
Sol	**Yes**	No	C	No license required	
FindBmcDevices	**No**	Yes	C/F	No license required	
FoundBmcDevices	No	**Yes**	F + C	No license required	
Shell	**Yes**	No	C	No license required	
Prompt	No	**Yes**	C	No license required	
Ch	**Yes**	No	C	No license required	

RemoteScreenVideo	**Yes**	**Yes**	F	SFT-DCMS-SINGLE	
[GPU Management]					
GetGpuInfo	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
UpdateGpu	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
DiagGpuStatus	**Yes**	**Yes**	C	**SFT-OOB-LIC**	
GetGpuLog	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
GpuPowerManage	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
[CPLD Management]					
GetCpldInfo	**Yes**	**Yes**	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	**SFT-DCMS-SINGLE**	
UpdateAomboardCpld	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
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	**SFT-DCMS-SINGLE**	
UpdateNICCpld	**Yes**	**Yes**	F	**SFT-DCMS-SINGLE**	
GetTransitionboardCpldInfo	**Yes**	**Yes**	C	No license required	
UpdateTransitionboardCpld	**Yes**	**No**	C	No license required	
[NIC Management]					
GetAocNICInfo	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
UpdatetAocNIC	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
[Multi-Node Management]					
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	
GetMultinodeLcmcInfo	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
UpdateMultinodeLcmc	**Yes**	**Yes**	C	**SFT-DCMS-SINGLE**	
[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	
SecureBoot Manage	**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	No license required	**For action Compare:** **• SFT-DCMS-SINGLE is required.** **• SFT-SDDC-SINGLE or SFT-SDLCR-NODE is required.**
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	**SFT-OOB-LIC**	
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	**SFT-DCMS-SINGLE is required for Recover and DownloadEvidence actions.**
[FPGA Management]					
GetMotherboardFpgaInfo	**Yes**	**Yes**	C	No license required	
UpdateMotherboardFpga	**Yes**	No	C	No license required	
[MCU Management]					

GetMotherboardMcuInfo	**Yes**	**Yes**	C	No license required	
UpdateMotherboardMcu	**Yes**	**Yes**	C	No license required	
[Switch Management]					
GetBladeSwitchInfo	**Yes**	No	F + C	No license required	
UpdateBladeSwitch	**Yes**	No	F + C	No license required	
RebootBladeSwitch	**Yes**	No	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 assiging 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 (MEIx64) is installed on Windows.
- The ChangeBiosCfg command will show error messages if the current BIOS configuration is different from the generated BIOS XML configuration file.
- BIOS XML configuration requires a text editor supporting extended ASCII characters (ISO-8859-1 encoding).
- 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 with the --address option only supports PSU “PWS-2K04A-1R” and “PWS-2K20A-1R.”
- The UpdatePsu command with the --address option does not support multiple OOB usages.
- The UpdatePsu command with the --index option supports only the PSU "PWS-5K26G-2R" on the H13DSG-OM system.

PCIeSwitch 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	8.15.0	MIT
saa	openssl	3.5.2	OpenSSL
saa	CryptoPP	5.6.2	Boost 1.0
saa	EDK2 Compress/ Decompress	EDK2	BSD
saa	Jsoncpp	1.8.4	MIT
phymem.sys/pmdll.dl	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	3.5.0	BSD 3-Clause
saa	Isocline	1.0.2	MIT
saa	LodePNG	20230410	zlib
saa	zlib	1.3.1	zlib

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

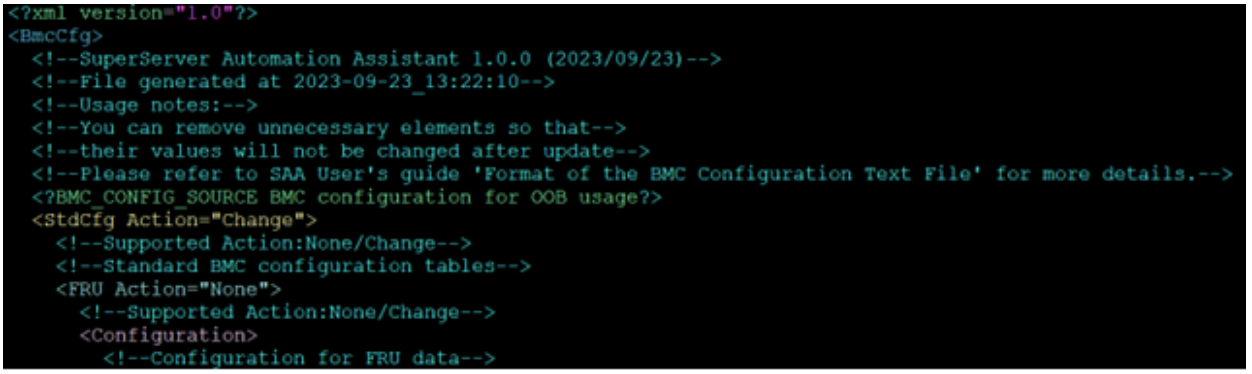
Use SAA and pair with the feature supported BIOS. You must ensure that the activated product key level is greater than or equal to the license requirement to change license required BIOS settings. You can query the existed product key by QueryProductKey command, see 5.1.2 Querying the Node Product Keys. 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)



- 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:

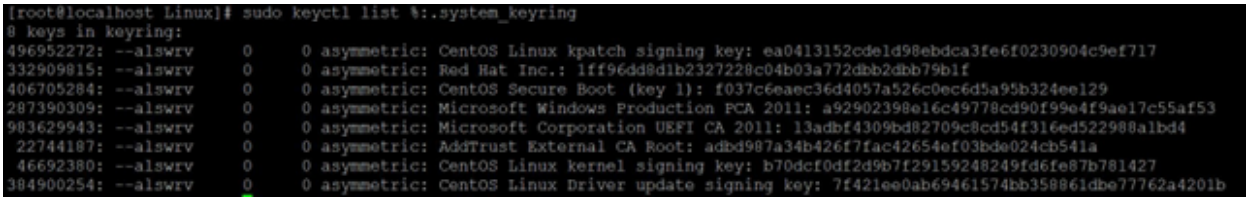
```
[root@localhost Linux]# sudo mokutil --sb-state
SecureBoot enabled
```

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:



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.

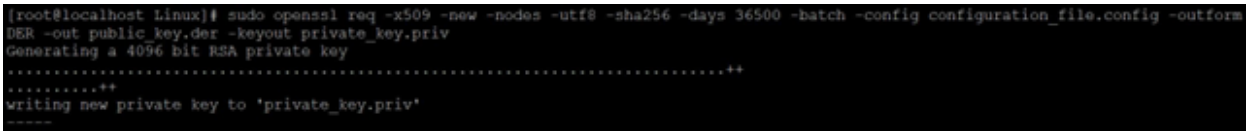
Syntax:

[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:



6. Add your public key to the MOK list by using Linux mokutil.

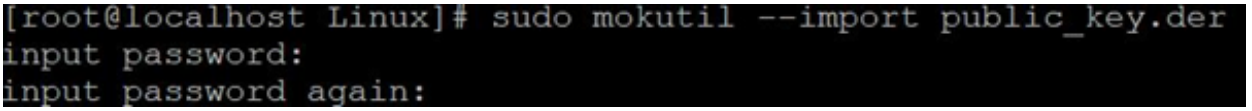
Syntax:

[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.

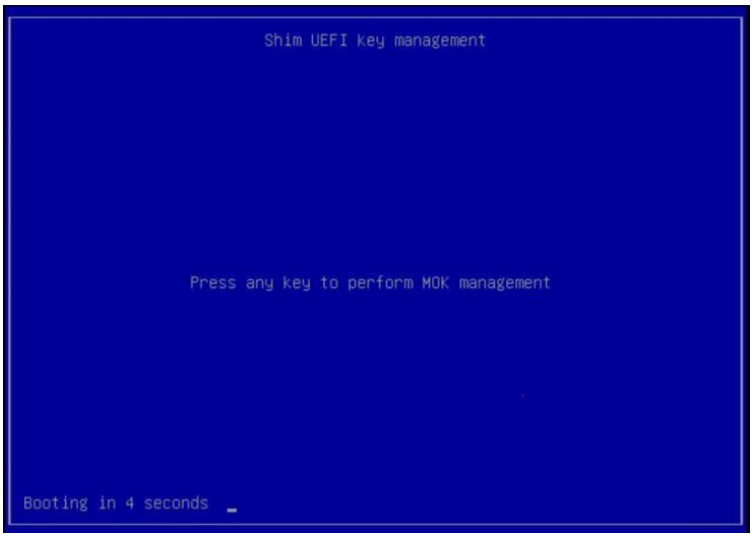
Example:



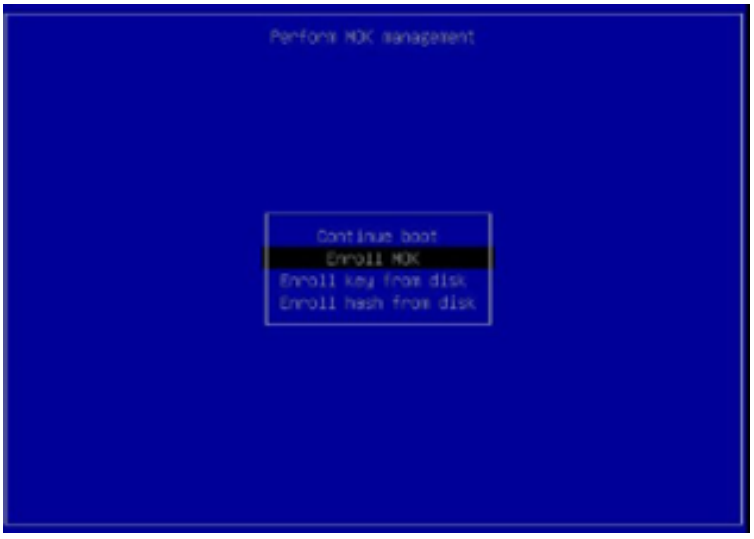
7. Reboot the system and enroll the key.

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.1.1 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.1.2 Ampere OpenBMC platforms

New password rules have been applied to Ampere OpenBMC 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 20 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
[BIOS Management]	
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	**Yes**
SetBootOption	No
SetHttpBoot	No
[BMC Management]	

UpdateBmc	No
GetBmcInfo	**Yes**
GetBmcCfg	**Yes**
ChangeBmcCfg	No
DownloadBmcCfg	**Yes**
UploadBmcCfg	No
SetBmcPassword	No
GetKcsPriv	**Yes**
SetKcsPriv	No
LoadDefaultBmcCfg	No
BmcReset	No
GetBmcUserList	**Yes**
SetBmcUserList	No
RmcpManage	**Yes**
GetSessionInfo	**Yes**
SessionManage	No
BmcWatchDog	No
SNMPManage	No
BmcIPv6StaticRouteManage	No
[System Event Log]	
GetEventLog	**Yes**
ClearEventLog	No
GetMaintenEventLog	**Yes**
ClearMaintenEventLog	No
GetHostDump	No
SetSELTimeMode	No
[CMM Management]	
UpdateCmm	No

GetCmmInfo	**Yes**
GetCmmCfg	**Yes**
ChangeCmmCfg	No
SetCmmPassword	No
LoadDefaultCmmCfg	No
GetBbpInfo	**Yes**
UpdateBbp	No
GetBladePowerStatus	**Yes**
SetBladePowerAction	No
BladePsuManage	**Yes**
BladeSummary	**Yes**
BladeConsole	No
GetBmcUserList	**Yes**
SetBmcUserList	No
UpdateDummySwitch	No
BladeNodeManage	**Yes**
[Storage Management]	
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**
[Power Management]	
GetPsuInfo	**Yes**
UpdatePsu	**No**
GetPowerStatus	**Yes**
SetPowerAction	**Yes**
DcmiManage	**Yes**
PowerPolicy	**No**
GetAcpiPowerStatus	**Yes**
GetPsFruInfo	**Yes**
CpuPowerManage	**No**
GetPowerShelfInfo	**Yes**
UpdatePowerShelf	**No**
[PCIeSwitch Management]	
GetPCIeSwitchInfo	**Yes**
UpdatePCIeSwitch	**No**
[Applications]	
RawCommand	**Yes**
GetUsbAccessMode	**Yes**
SetUsbAccessMode	**No**
KmsManage	**No**
RedfishApi	**Yes**
RemoteExec	**Yes**
RemoteConsole	**No**
RemoteScreenshot	**No**
RemoteKeyboard	**No**

Sol	No
FindBmcDevices	**Yes**
Shell	**Yes**
Prompt	**Yes**
Ch	**Yes**
RemoteScreenVideo	No
[GPU Management]	
GetGpuInfo	**Yes**
UpdateGpu	No
DiagGpuStatus	**Yes**
GetGpuLog	No
GpuPowerManage	No
[CPLD Management]	
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
[NIC Management]	
GetAocNICInfo	**Yes**
UpdatetAocNIC	No
[Multi-Node Management]	
GetTpInfo	**Yes**
ChangeTpInfo	No
GetMultinodeEcInfo	**Yes**
UpdateMultinodeEc	No
GetMultinodeLcmcInfo	**Yes**
UpdateMultinodeLcmc	No
[VM Management]	
MountIsoImage	No
UnmountIsoImage	No
MountFloppyImage	No
UnmountFloppyImage	No
GetVmInfo	**Yes**
VmManage	No
VMShell	No
[NM Management]	
NmMeManage	No
GeneralNmManage	No
NmCpuManage	No
NmCupsManage	No

BmcNmManage	**Yes**
[Security Management]	
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**
CertManage	**Yes**
[FPGA Management]	
GetMotherboardFpgaInfo	**Yes**
UpdateMotherboardFpga	No
[MCU Management]	

GetMotherboardMcuInfo	**Yes**
UpdateMotherboardMcu	**No**
[Switch Management]	
NvSwitchManage	**Yes**
GetBladeSwitchInfo	**Yes**
UpdateBladeSwitch	**Yes**
RebootBladeSwitch	**Yes**

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 nvmupdate64e && ./LLDP_EN.sh"

1. The file STGF2S3B3_NUP.zip on the managing system is copied to the /tmp/STGF2S3B3_NUP.zip path on the remote system.
2. The working directory is changed to /tmp/ to access the files under /tmp/ in a relative path.
3. The “unzip -o STGF2S3B3_NUP.zip” file uncompresses and overwrites the existing files.
4. The working directory is changed to STGF2S3B3_NUP.
5. Both “chmod +x LLDP_EN.sh” and “chmod +x nvmupdate64e” files make the files executable.
6. LLDP_EN(.sh) is an update script from the vendor, nvmupdate64e is the binary to update the firmware, and nvmupdate.cfg is the configuration file required for nvmupdate64e. The “./LLDP_EN.sh” file will call nvmupdate64e with nvmupdate.cfg (relative path in STGF2S3B3_NUP) to update the NIC firmware.

K.2 NVIDIA HGX A100 GPU firmware update package

The main updating GPU firmware package consists of two particular packages. One is script package named as A100_v1.0 and the other is vendor package named as HGX_A100_8-GPU_80G_AC_Firmware_22.05.03.

Both packages are designated for NVIDIA HGX A100 systems with 40 or 80GB memory size GPU firmware updating.

The script package contains scripts and config.txt. 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

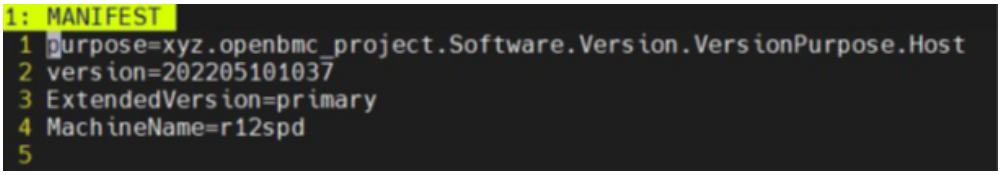
L.1 BIOS Firmware Updating Tar File for OpenBMC

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
```



2. Create a tar file including the firmware image and MAINFEST file:

```
$ tar -cvf bios_image.tar bios_image MANIFEST
```

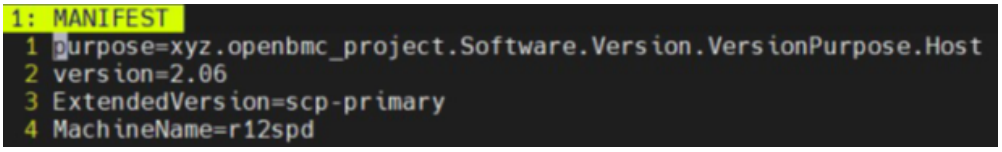
L.2 Ampere SCP Firmware Updating Tar File for OpenBMC

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
```



2. Create a tar file including the firmware image and MAINFEST file:

```
$ tar -cvf r12spd_atf_xxxx.tar altra_scp_signed_x.xx.xxxxx.slim MANIFEST
```

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
PowerShelf	GetPowerShelfInfo	UpdatePowerShelf	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
Multinode LCMC	GetMultinodeLcmcInfo	UpdateMultinodeLcmc	N/A

Backplane storage CPLD	GetBackplaneCpldInfo	UpdateBackplaneCpld	N/A
PCIe Switch	GetPCIeSwitchInfo	UpdatePCIeSwitch	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
CPU ERoT	GetCpuERotInfo	UpdateCpuERot	CpuERotManage

Appendix N. GetGpuInfo/UpdateGpu supported platform matrix

Here is the table of GPU platforms mapping with Supermicro product SKUs and GetGpuIfno 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	GetPcieSwitchinfo/UpdatePcieSwitch
Intel PVC	SYS-821GV-TNR	V	V	4xPEX89104:Synthetic mode + 2xPEX89072:Base mode
Intel Gaudi 2	SYS-820GH-TNR2	V	V	X
Intel Gaudi 3	SYS-822GA-NGR3	V	V	2xPLX89144:Synthetic mode
Nvidia H100/H200 Delta Next	• SYS-821GE-TNHR • AS-8125GS-TNHR	V	V	4xPEX89104:Synthetic mode + 2xPEX89072:Base mode
Nvidia A100 Delta	• SYS-420GP-TNAR • AS-4124GO-NART	V	V	4xPEX88096:Base mode
Nvidia H100 Redstone Next	• SYS-21GE-TNHT-LCC • SYS-421GU-TNXR	V	V	X
Nvidia A100 Redstone	• SYS-421GU-TNXR • SYS-420GU-TNXR	V	X (*See Note*)	X

	• SYS-220GQ-TNAR • AS-2124GQ-NART			
Nvidia HGX B200	• SYS-422GA-NBRT-LCC • SYS-A22GA-NBRT	V	V	4xPEX89144:Synthetic mode
Nvidia HGX B300	• SYS-822GS-NB3RT • AS-8126GS-NB3RT	V	V	4xPEX89144:Synthetic mode
Nvidia HGX GB200	• ARS-121GL-NBO	V	V	X
Nvidia HGX GB300	• ARS-121GL-NB3-LCC	V	V	X
AMD MI300X	• AS-8125GS-TNMR2 • SYS-821GE-TNMR2	V	V	4xPEX89104:Synthetic mode + 2xPEX89072:Base mode
AMD MI325X/MI355X	• AS-4126GS-NMR-LCC	V	V	X
Nvidia MGX	• ARS-111GL-NHR	V	V	X



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 (Showing info for IFWI and PSCBIN)	V (supported --item = {PVC_IFWI,PVC_PSCBIN})
	OOB/Inband RHI	V (Showing info for AMC, UBB CPLD and Retimer)	V (supported --item = {PVC_AMC,PVC_UBB_CPLD,PVC_RETIMER})
Intel Gaudi 2	In-Band	V (Showing info for SPI, OAM CPLD UBB CPLD)	V (supported --item = {GAUDI_SPI,GAUDI_OAM_CPLD,GAUDI_UBB_CPLD})
	OOB/Inband RHI	V (Showing info for Retimer)	V (supported --item = {GAUDI_RETIMER})
Intel Gaudi 3	In-Band	V (Showing info for SPI, OAM CPLD)	V (supported --item = {GAUDI_SPI,GAUDI_OAM_CPLD})
	OOB/Inband RHI	V (Showing info for UBB CPLD, UBB CPLD2 and Retimer)	V (supported --item = {GAUDI_UBB_CPLD,GAUDI_UBB_CPLD2,GAUDI_RETIMER})
Nvidia A100 Delta	In-Band	X	X
	OOB/Inband RHI	V	V (supported --item = {CEC,FPGA})
Nvidia A100 Redstone	In-Band	X	X
	OOB/Inband RHI	V	X
Nvidia HGX Delta-Next	In-Band	X	X
	OOB/Inband RHI	V	V (supported --item = {HGX,HGX_FPGA,HGX_HMC,HGX_HMC_EROT,HGX_FPGA_EROT,HGX_PCIESWITCH,HGX_PCIESWITCH_EROT,HGX_GPU,,HGX_GPU

			_EROT,HGX_NVSWITCH,HGX_NVSWITCH_EROT,HGX_RETIMER})
Nvidia HGX Redstone Next	In-Band	X	X
	OOB/Inband RHI	V	V (supported --item = {HGX_FPGA,HGX_GPU})
Nvidia HGX B200	In-Band	X	X
	OOB/Inband RHI	V	V (supported --item = {HGX,HGX_FPGA,HGX_HMC,HGX_HMC_EROT,HGX_FPGA_EROT,HGX_GPU,HGX_GPU_EROT,HGX_NVSWITCH,HGX_NVSWITCH_EROT,HGX_RETIMER,HGX_NVLINKMANAGEMENTNIC,HGX_NVLINKMANAGEMENTNIC_EROT})
Nvidia HGX B300	In-Band	X	X
	OOB/Inband RHI	V	V (supported --item = {HGX,HGX_FPGA,HGX_HMC,HGX_HMC_EROT,HGX_FPGA_EROT,HGX_GPU,HGX_GPU_EROT,HGX_NVSWITCH,HGX_NVSWITCH_EROT,HGX_NVLINKMANAGEMENTNIC,HGX_NVLINKMANAGEMENTNIC_EROT})
Nvidia HGX GB200/GB300	In-Band	X	X
	OOB/Inband RHI	V	V (supported --item = {HGX,HGX_HMC,HGX_HMC_EROT,HGX_FPGA,HGX_FPGA_EROT,HGX_GPU,HGX_CPU,HGX_CPU_EROT,HGX_CP

			LD,HGX_GPU_INFOROM,})
AMD MI300X/MI325X/MI355X	In-Band	X	X
	OOB/Inband RHI	V	V (supported --item = {MI300X})
Nvidia MGX	In-Band	X	X
	OOB/Inband RHI	V	V (supported --item = {MGX_GPU})

Appendix O. Power Capping

O.1 Introduction

Power Capping serves to limit the maximum power consumption of a managed system, ensuring stability and preventing the system from exceeding power or thermal limits. This approach helps maintain reliable operation while optimizing energy use.

O.2 Power Capping Methods

Below are the purposes and power capping methods for different SAA commands:

Command	Purpose	Power Capping Method	Supported Platform
GeneralNmManage	Comprehensive system management (incl. Get NM version, manage power budget)	Directly limits maximum system power consumption via power budget management	Intel platform with Node Manager support
PowerPolicy	Dynamic power adjustments based on system power policies	Automatically adjusts when power exceeds budget via predefined policies	Intel platform with Node Manager support
DcmiManage	Standardized power capping for data center environments using DCMI	Enforces power limits by throttling components when exceeded	Intel platform with Node Manager support
ChangeBmcCfg (SmartPower configuration)	Adaptive power optimization based on system load, power consumption, and thermal conditions	Dynamically redistributes power based on real-time system status without requiring pre-defined policies	Please contact a Supermicro sales representative or technical support for information on Smart Power-supported platforms.

Notes:

- The PowerPolicy command is used for creating and managing power policies, while the decision-making and execution of these policies

are controlled by Node Manager (NM).

- While the PSys domain is required for system-level power capping in Node Manager (NM), power capping is still supported even if the managed system lacks PSys. This is achieved through the CPU and memory domains using the PowerPolicy and GeneralNmManage commands.

O.3 Scenario Example

In each scenario example, the initial step is to set the power budget. You can use the GeneralNmManage command to establish an overall power budget for the system, such as 1000 W.

```
# ./saa -c GeneralNmManage --type NM20 –action SetTotalPower --value 1000 --
domain_id 0
```

O.3.1 Scenario Example for PowerPolicy Command

1. Set Power Policies: You can use the PowerPolicy command to set different power policies for the system, including high-performance mode, balanced mode, and energy-saving mode.

- High-performance mode: You can set higher power limits, allowing the system to operate at higher frequencies and achieve higher performance. The power limits in this mode can be set to 1000 W or close to 1000 W.

```
# ./saa -c PowerPolicy --type NM20 --action AddPolicy --domain_id 0 --policy_id 1
--trigger_type 0 --mode 0 --exception_action 1 --limit 800 --time 20000 --
trigger_limit 1000 --period 200 --overwrite
```

- Balanced mode: You can set medium power limits to balance performance and power consumption, such as 700 W.

```
# ./saa -c PowerPolicy --type NM20 --action AddPolicy --domain_id 0 --policy_id 2
--trigger_type 0 --mode 0 --exception_action 1 --limit 500 --time 20000 --
```

```
trigger_limit 700 --period 200 --overwrite
```

- Energy-saving mode: Set lower power limits to reduce system frequency, thereby reducing energy consumption, such as 500 W.

```
# ./saa -c PowerPolicy --type NM20 --action AddPolicy --domain_id 0 --policy_id 3
--trigger_type 0 --mode 0 --exception_action 1 --limit 200 --time 20000 --
trigger_limit 500 --period 200 --overwrite
```

2. Dynamic Adjustment: The Node Manager applies the optimal power policy based on real-time workloads and system conditions. For example:

- High workload: Node Manager switches to high-performance mode to maintain application performance.
- Low workload: Node Manager switches to energy-saving mode to minimize power consumption.

O.3.2 Scenario Example for DcmiManage Command

1. Set Power Limit: You can configure a fixed power limit (e.g., 500 W) to prevent the system's power consumption from exceeding a defined threshold.

```
# ./saa -c DcmiManage --type NM20 --action SetPowerLimit --exception_action 1 --
limit 500 --time 20000 --period 50
```

2. Throttling Adjustment: When the system exceeds the power limit, DCMI throttles components to maintain power usage within the limit. The limit remains fixed, without dynamic adjustments based on workload.

O.3.3 Scenario Example for ChangeBmcCfg Command

1. Adaptive Smart Power Management: Dynamically adjusts power distribution in response to real-time system load, temperature, and power consumption. To enable this, set the "SmartPower" field to "SmartPowerModeOn" in the BMC configuration and then execute the ChangeBmcCfg command.

```
<?xml version="1.0"?>
<BmcCfg>
  <OemCfg Action="Change">
    <PowerSupply Action="Change">
      <!--Supported Action:None/Change-->
      <Information>
        <!--Information of the total power state on the system-->
        <TotalMaxPower>2200</TotalMaxPower>
        <!--Total maximum power. Unit in Watt(W)-->
        <TotalPowerConsumption>6</TotalPowerConsumption>
        <!--Total power consumption. Unit in Watt(W)-->
        <TotalPowerCapping>0</TotalPowerCapping>
        <!--Total capping power. Unit in Watt(W)-->
      </Information>
      <Configuration>
        <SmartPower>SmartPowerModeOn</SmartPower>
        <!--SmartPowerModeOn/SmartPowerModeOff-->
        <!--Smart power manages the power budget and limitation for all nodes on
the system.-->
        <!--Enable it to adjust power capping policy in case of exceeding power
capability.-->
        <!--HPC N-Power Mode is only supported in FlexTwin MB platform.-->
      </Configuration>
    </PowerSupply>
  </OemCfg>
</BmcCfg>
```

```
# ./saa -c ChangeBmcCfg --file BmcCfg.xml
```

2. Dynamic Adjustment: Unlike fixed limits, Smart Power continuously optimizes power consumption to maximize performance while minimizing power usage, adapting to real-time system conditions.



Note:

- If both power policy and smart power are configured in the managed system, the first to trigger will take priority. For example, if the power policy is set to 900 W and smart power is set to 800 W, smart power will be prioritized, as it will trigger first.

O.4 Summary

The GeneralNmManage command defines the power ceiling, while the PowerPolicy and DcmiManage commands, along with the Smart Power feature in the BMC configuration, dynamically manage power below it, dynamically manage power below it, allowing for more sophisticated and flexible power management.

Appendix P. How to Mount an ISO Image and Set It as a Boot Option

P.1 Introduction

If you want to mount an ISO Image and set it as a boot option, please refer to the following SAA commands:

1. VmManage/MountIsoImage: Mount an ISO image to virtual media from a remote server (supports Samba, HTTP, and HTTPS servers).
   - If the managed system supports multiple virtual media devices via the Redfish API, the user can use the VmManage command to mount an ISO image on a specified virtual media device.
   - If the managed system only supports a single virtual media device via the Redfish API, the user can use the MountIsoImage command to mount an ISO image on virtual media device 1.
2. SetBootOption: Set the boot option to boot from the ISO image and reboot the system.



Notes:

- Starting from platforms X12/H12 and later, BMC supports multiple virtual media management with newer BMC firmware via the Redfish API.
- To check if the managed system supports multiple virtual media management, please refer to GetVmInfo command.
  - If supported, this command will display detailed virtual media device information as shown below.

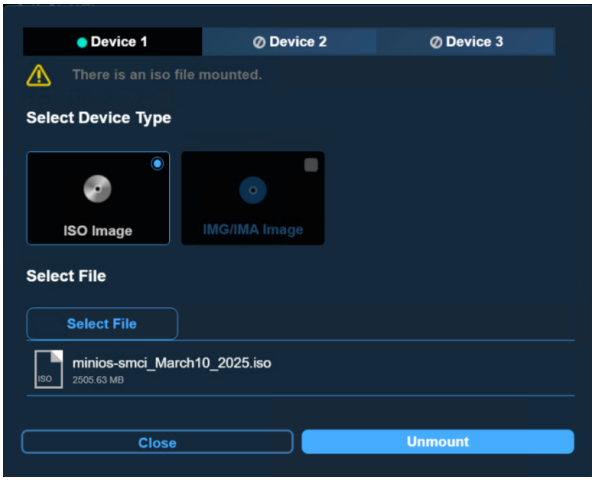
```
...
Virtual Media Device Information
============================
    Device 1
    ============
        Device status: Unmounted
        Media type: N/A
        Connection setting: NotConnected
        Image: N/A
        SSL certificate verified: N/A
        Self-signed certificate accepted: N/A
```

```
        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
...
```

  - If not supported, only the device status will be displayed, as shown below.

```
...
Virtual Media Device Information
============================
    Device 1: Empty device
    Device 2: Empty device
    Device 3: Empty device
```

- If the virtual media device is mounted via the remote console on the BMC web, as shown below, the SAA command cannot be used to manage the virtual media.



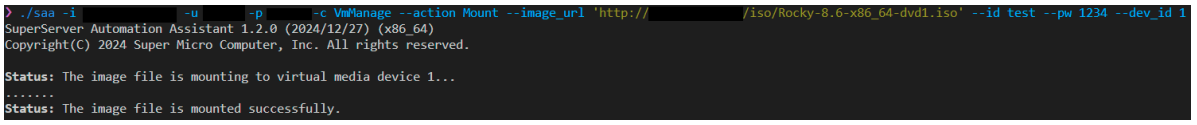
P.2 Example

The following are test steps using SAA commands, with the X13 platform as an example.

1. Mount the Rocky Linux 8 installer ISO image from a remote server to device 1.
   - Command usage

```
# ./saa -i <BMC IP> -u <BMC username> -p <BMC password> -c VmManage --action
Mount --image_url <Image URL> --id <Server ID> --password <Server password> -
-dev_id <Device ID>
```

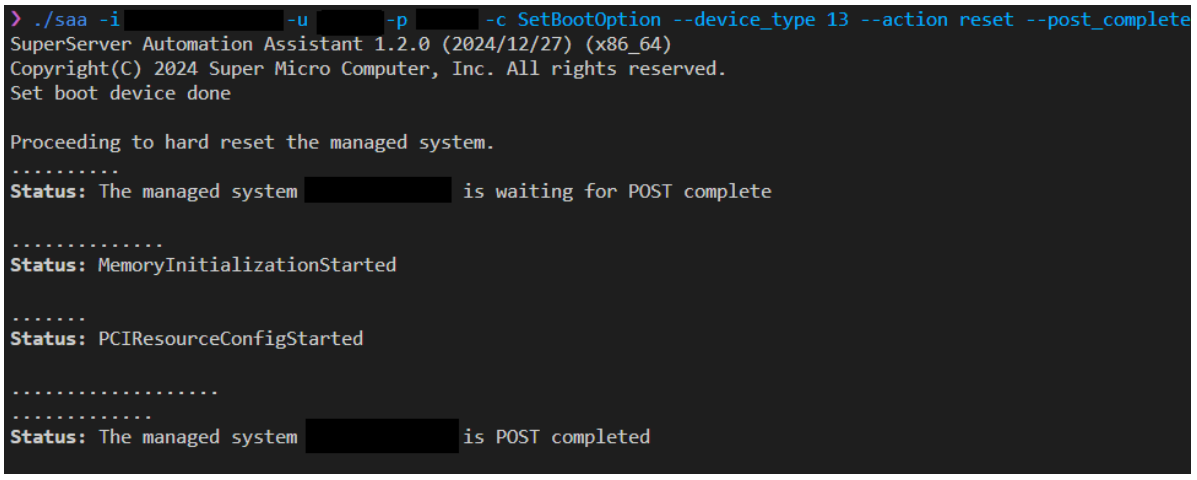
   - Command output



2. Set the boot option to "UEFI: ISO Image" (Device type = 13) and reboot the managed system.
   - Command usage

```
# ./saa -i <BMC IP> -u <BMC username> -p <BMC password> -c SetBootOption --
device_type 13 --action reset --post_complete
```

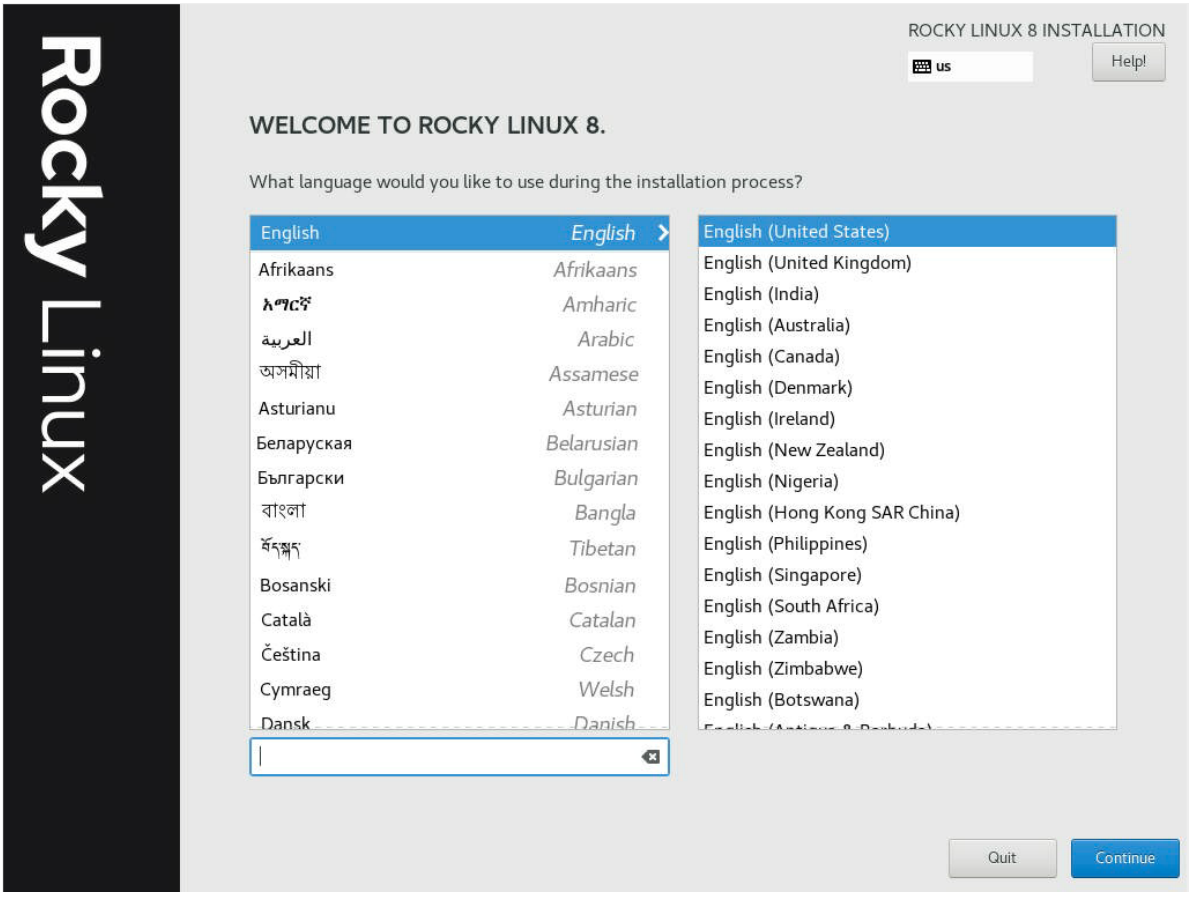
   - Command output



3. Check if the managed system booted into the ISO image mounted via the SAA command.



4. Access the Rocky Linux setup page.



Appendix Q. Sample Configuration Tables for BMC and CMM

The XML templates in this appendix demonstrate standard configurations for BMC and CMM systems. Use these as starting points for your deployments, modifying parameters to match your hardware and network environment.

The complete configuration files can be found in the SAA package.
You can find them in: `SampleFile/Configuration/`.

Important: These samples may not exactly match your environment. Modify them as needed before applying with the ChangeBmcCfg or ChangeCmmCfg command.

To create a configuration file that fits your system:

1. Execute the GetBmcCfg (for BMC) or GetCmmCfg (for CMM) command to retrieve the system's current XML configuration.
2. Edit the generated XML file to suit your specific requirements.

Q.1 Sample Configuration Tables

Q.1.1 Sample BMC Configuration Table

The sample BMC configuration tables below are from X14 platforms.

Q.1.1.1 Account Management

Account management controls local BMC users, privileges, and password policy behavior.

- Table Type: In-Band
  - Table Name: UserManagement
  - XPath: `BmcCfg/StdCfg/UserManagement`
  - Sample XML Format:

```
<BmcCfg>
  <StdCfg Action="Change">
```

```
    <UserManagement Action="Change">
      <Information>
        <MaximumAvailableIDs>16</MaximumAvailableIDs>
        <TotalIDEnabled>1</TotalIDEnabled>
      </Information>
      <Configuration>
        <User UserID="2">
          <Access>Enable</Access>
          <Name><![CDATA[ADMIN]]></Name>
          <Password><![CDATA[]]></Password>
          <PrivilegeLimit>Administrator</PrivilegeLimit>
          <SOLAccess>Enable</SOLAccess>
        </User>
      </Configuration>
    </UserManagement>
  </StdCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: Account
  - XPath: `BmcCfg/OemCfg/Account`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <Account Action="Change">
      <Information>
        <MaximumAvailableIDs>16</MaximumAvailableIDs>
        <TotalIDEnabled>1</TotalIDEnabled>
      </Information>
      <Configuration>
        <AccountLockoutThreshold>3</AccountLockoutThreshold>

<AccountLockoutCounterResetAfter>30</AccountLockoutCounterResetAfter>
        <AccountLockoutDuration>30</AccountLockoutDuration>
        <User Action="Change" UserID="2">
          <Configuration>
            <UserName><![CDATA[ADMIN]]></UserName>
            <Password><![CDATA[]]></Password>
            <RoleId>Administrator</RoleId>
            <Locked>false</Locked>
            <Enabled>Enable</Enabled>
            <AccountTypes>Redfish,IPMI</AccountTypes>
            <SNMP Action="Change">
              <Configuration>
                <AuthenticationProtocol>HMAC_MD5</AuthenticationProtocol>
                <EncryptionProtocol>CBC_DES</EncryptionProtocol>
                <AuthenticationKey></AuthenticationKey>
                <EncryptionKey></EncryptionKey>
              </Configuration>
            </SNMP>
```

```
          </Configuration>
        </User>
      </Configuration>
    </Account>
  </OemCfg>
</BmcCfg>
```

Q.1.1.2 AD Management

Active Directory (AD) integration allows the BMC authenticate users through Microsoft AD domains instead of local accounts.

- Table Type: OOB
  - Table Name: AD
  - XPath: `BmcCfg/OemCfg/AD`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <AD Action="Overwrite">
      <Information>
        <MaximumAvailableADGroup>5</MaximumAvailableADGroup>
        <TotalConfiguredADGroup>0</TotalConfiguredADGroup>
        <DynamicServerAddress1></DynamicServerAddress1>
        <DynamicServerAddress2></DynamicServerAddress2>
        <DynamicServerAddress3></DynamicServerAddress3>
        <DynamicServerAddress4></DynamicServerAddress4>
        <DynamicServerAddress5></DynamicServerAddress5>
      </Information>
      <Configuration>
        <ADEnable>Disable</ADEnable>
        <DNSLookupEnable>Disable</DNSLookupEnable>
        <Prefix>ldap</Prefix>
        <Port>389</Port>
        <UserDomainName1></UserDomainName1>
        <UserDomainName2></UserDomainName2>
        <UserDomainName3></UserDomainName3>
        <UserDomainName4></UserDomainName4>
        <UserDomainName5></UserDomainName5>
        <ServiceAddr1></ServiceAddr1>
        <ServiceAddr2></ServiceAddr2>
        <ServiceAddr3></ServiceAddr3>
        <ADRule Action="Change" RuleID="1">
          <Configuration>
            <RemoteUser><![CDATA[]]></RemoteUser>
            <RemoteGroup><![CDATA[]]></RemoteGroup>
            <RulePrivilege>None</RulePrivilege>
          </Configuration>
```

```
        </ADRule>
      </Configuration>
    </AD>
  </OemCfg>
</BmcCfg>
```

Q.1.1.3 LDAP Management

LDAP integration enables authentication of BMC logins against an external LDAP directory service.

- Table Type: OOB
  - Table Name: LDAP
  - XPath: `BmcCfg/OemCfg/LDAP`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <LDAP Action="Overwrite">
      <Information>
        <MaximumAvailableADGroup>5</MaximumAvailableADGroup>
        <TotalConfiguredADGroup>0</TotalConfiguredADGroup>
      </Information>
      <Configuration>
        <LDAPEnable>Disable</LDAPEnable>
        <BindDN></BindDN>
        <BindPassword></BindPassword>
        <UsernameAttribute></UsernameAttribute>
        <GroupsAttribute></GroupsAttribute>
        <SearchBase1></SearchBase1>
        <SearchBase2></SearchBase2>
        <SearchBase3></SearchBase3>
        <ServiceAddr1></ServiceAddr1>
        <ServiceAddr2></ServiceAddr2>
        <ServiceAddr3></ServiceAddr3>
        <LDAPRule Action="Change" RuleID="0">
          <Configuration>
            <RemoteUser><![CDATA[]]></RemoteUser>
            <RemoteGroup><![CDATA[]]></RemoteGroup>
            <RulePrivilege>None</RulePrivilege>
          </Configuration>
        </LDAPRule>
      </Configuration>
    </LDAP>
  </OemCfg>
</BmcCfg>
```

Q.1.1.4 RADIUS Management

RADIUS authentication allows the BMC to validate user credentials through an external RADIUS server.

- Table Type: In-Band
  - Table Name: RADIUS
  - XPath: `BmcCfg/OemCfg/RADIUS`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <RADIUS Action="Change">
      <Configuration>
        <RADIUSEnable>Disable</RADIUSEnable>
        <Port>1812</Port>
        <ServerAddress>0.0.0.0</ServerAddress>
        <Secret></Secret>
      </Configuration>
    </RADIUS>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: RADIUS
  - XPath: `BmcCfg/OemCfg/RADIUS`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <RADIUS Action="Overwrite">
      <Configuration>
        <RADIUSEnable>Disable</RADIUSEnable>
        <Port>1812</Port>
        <ServerAddress>0.0.0.0</ServerAddress>
        <Secret></Secret>
      </Configuration>
    </RADIUS>
  </OemCfg>
</BmcCfg>
```

Q.1.1.5 Advance Event Log Management

The Advanced Event Log records additional system events such as AC-power-on for system auditing.

- Table Type: In-Band
  - Table Name: AdvanceEventLog
  - XPath: `BmcCfg/OemCfg/AdvanceEventLog`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <AdvanceEventLog Action="Change">
      <Configuration>
        <ACPowerOnEventLog>Enable</ACPowerOnEventLog>
      </Configuration>
    </AdvanceEventLog>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: AdvanceEventLog
  - XPath: `BmcCfg/OemCfg/AdvanceEventLog`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <AdvanceEventLog Action="Change">
      <Configuration>
        <ACPowerOnEventLog>Enable</ACPowerOnEventLog>
      </Configuration>
    </AdvanceEventLog>
  </OemCfg>
</BmcCfg>
```

Q.1.1.6 Alert Management

The Alert List defines where and how the BMC sends event notifications by SNMP, SMTP or Redfish.

- Table Type: OOB
  - Table Name: AlertList
  - XPath: `BmcCfg/OemCfg/AlertList`

- Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <AlertList Action="Change">
      <Information>
        <MaximumAvailableAlerts>16</MaximumAvailableAlerts>
        <TotalConfiguredAlerts>0</TotalConfiguredAlerts>
      </Information>
      <Configuration>
        <Alert Action="Change" AlertNumber="1">
          <Configuration>
            <Enable>Disable</Enable>
            <Protocol>SNMPv1</Protocol>
            <EventType></EventType>
            <Destination>snmp://0.0.0.0</Destination>
            <Severity>Information</Severity>
            <TrapCommunity></TrapCommunity>
            <MailMessage></MailMessage>
            <MailSubject></MailSubject>
            <UserName></UserName>
            <AuthenticationKey></AuthenticationKey>
            <AuthenticationProtocol>HMAC_MD5</AuthenticationProtocol>
            <EncryptionKey></EncryptionKey>
            <EncryptionProtocol>CBC_DES</EncryptionProtocol>
          </Configuration>
        </Alert>
      </Configuration>
    </AlertList>
  </OemCfg>
</BmcCfg>
```

Q.1.1.7 BOOT Management

Boot settings specify the next-boot mode, device and whether to bypass passwords after a power cycle.

- Table Type: In-Band
  - Table Name: BOOT
  - XPath: `BmcCfg/StdCfg/BOOT`
  - Sample XML Format:

```
<BmcCfg>
  <StdCfg Action="Change">
    <BOOT Action="Change">
      <Configuration>
        <NextBootOnly>Enable</NextBootOnly>
```

```
        <BypassPassword>Disable</BypassPassword>
        <BootMode>Legacy</BootMode>
        <LegacyDeviceType>No Override</LegacyDeviceType>
        <UEFIDeviceType>No Override</UEFIDeviceType>
      </Configuration>
    </BOOT>
  </StdCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: BOOT
  - XPath: `BmcCfg/StdCfg/BOOT`
  - Sample XML Format:

```
<BmcCfg>
  <StdCfg Action="Change">
    <BOOT Action="Change">
      <Configuration>
        <NextBootOnly>Enable</NextBootOnly>
        <BypassPassword>Disable</BypassPassword>
        <BootMode>Legacy</BootMode>
        <LegacyDeviceType>No Override</LegacyDeviceType>
        <UEFIDeviceType>No Override</UEFIDeviceType>
      </Configuration>
    </BOOT>
  </StdCfg>
</BmcCfg>
```

Q.1.1.8 Certification Management

The Certificate management allows administrators to upload custom SSL certificates and keys for secure HTTPS and Redfish access.

- Table Type: In-Band
  - Table Name: Certification
  - XPath: `BmcCfg/OemCfg/Certification`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <Certification Action="Change">
      <Information>
        <CertStartDate>May  2 00:00:00 2025 GMT</CertStartDate>
        <CertEndDate>May  2 00:00:00 2028 GMT</CertEndDate>
      </Information>
```

```
      <Configuration>
        <CertFile></CertFile>
        <PrivKeyFile></PrivKeyFile>
      </Configuration>
    </Certification>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: Certification
  - XPath: `BmcCfg/OemCfg/Certification`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <Certification Action="Change">
      <Information>
        <CertStartDate>May  2 00:00:00 2025 GMT</CertStartDate>
        <CertEndDate>May  2 00:00:00 2028 GMT</CertEndDate>
      </Information>
      <Configuration>
        <CertFile></CertFile>
        <PrivKeyFile></PrivKeyFile>
      </Configuration>
    </Certification>
  </OemCfg>
</BmcCfg>
```

Q.1.1.9 DateTime Management

Date & Time sets the BMC clock, timezone, daylight-saving and optional NTP servers.

- Table Type: In-Band
  - Table Name: DateTime
  - XPath: `BmcCfg/OemCfg/DateTime`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <DateTime Action="Change">
      <Information>
        <DateTimeValue>2024/10/9 14:39</DateTimeValue>
      </Information>
      <Configuration>
        <TimeUpdateMode>Local</TimeUpdateMode>
        <NTPPrimaryServer>localhost</NTPPrimaryServer>
```

```
        <NTPSecondaryServer>127.0.0.1</NTPSecondaryServer>
        <TimeZone>(UTC+00:00) Coordinated Universal Time</TimeZone>
        <AutoDSTEnabled>Disable</AutoDSTEnabled>
      </Configuration>
    </DateTime>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: DateTime
  - XPath: `BmcCfg/OemCfg/DateTime`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <DateTime Action="Change">
      <Information>
        <DateTime>2024/10/9 14:19</DateTime>
        <DateTimeLocalOffset>+00:00</DateTimeLocalOffset>
      </Information>
      <Configuration>
        <NTPEnable>Disable</NTPEnable>
        <PrimaryNTPServer>localhost</PrimaryNTPServer>
        <SecondaryNTPServer>127.0.0.1</SecondaryNTPServer>
        <TimeZone>(UTC+00:00) Coordinated Universal Time</TimeZone>
        <AutoDSTEnabled>Disable</AutoDSTEnabled>
      </Configuration>
    </DateTime>
  </OemCfg>
</BmcCfg>
```

Q.1.1.10 Dynamic DNS Management

The Dynamic DNS (DDNS) allows the BMC to register its hostname automatically when its IP address changes.

- Table Type: In-Band
  - Table Name: DDNS
  - XPath: `BmcCfg/OemCfg/DDNS`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <DDNS Action="Change">
      <Configuration>
```

```
        <DDNSEnable>Disable</DDNSEnable>
        <TSIGEnable>Disable</TSIGEnable>
        <ServerIP>0.0.0.0</ServerIP>
        <BMCHostName></BMCHostName>
        <?Note Will be skipped in multiple system usage without --
individually option.?>
        <TSIGPubKeyFile></TSIGPubKeyFile>
        <TSIGPrivKeyFile></TSIGPrivKeyFile>
      </Configuration>
    </DDNS>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: DDNS
  - XPath: `BmcCfg/OemCfg/DDNS`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <DDNS Action="Change">
      <Configuration>
        <DDNSEnable>Disable</DDNSEnable>
        <TSIGEnable>Disable</TSIGEnable>
        <ServerIP>0.0.0.0</ServerIP>
        <BMCHostName></BMCHostName>
        <?Note Will be skipped in multiple system usage without --
individually option.?>
        <TSIGPubKeyFile></TSIGPubKeyFile>
        <TSIGPrivKeyFile></TSIGPrivKeyFile>
      </Configuration>
    </DDNS>
  </OemCfg>
</BmcCfg>
```

Q.1.1.11 Device Control Management

The Device Control adjusts hardware behavior such as fan profiles or power modes to balance cooling and acoustics.

- Table Type: In-Band
  - Table Name: DeviceControl
  - XPath: `BmcCfg/OemCfg/DeviceControl`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <DeviceControl Action="Change">
      <Configuration>
        <FanMode>Optimal</FanMode>
      </Configuration>
    </DeviceControl>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: DeviceControl
  - XPath: `BmcCfg/OemCfg/DeviceControl`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <DeviceControl Action="Change">
      <Configuration>
        <FanMode>Optimal</FanMode>
      </Configuration>
    </DeviceControl>
  </OemCfg>
</BmcCfg>
```

Q.1.1.12 FRU Management

The Field Replaceable Unit (FRU) stores manufacturing, serial-number and part information for board, chassis and product identification.

- Table Type: In-Band
  - Table Name: FRU
  - XPath: `BmcCfg/StdCfg/FRU`
  - Sample XML Format:

```
<BmcCfg>
  <StdCfg Action="Change">
    <FRU Action="Change">
      <Configuration>
        <BoardMfgDateTime>1996/1/1 0:0</BoardMfgDateTime>
        <BoardMfgName></BoardMfgName>
        <BoardProductName></BoardProductName>
        <BoardSerialNum></BoardSerialNum>
        <BoardPartNum></BoardPartNum>
```

```
        <ProductMfgName></ProductMfgName>
        <ProductName></ProductName>
        <ProductPartModelNum></ProductPartModelNum>
        <ProductVersion></ProductVersion>
        <ProductSerialNum></ProductSerialNum>
        <ProductAssetTag></ProductAssetTag>
        <ChassisType>0x0</ChassisType>
        <ChassisPartNumber></ChassisPartNumber>
        <ChassisSerialNumber></ChassisSerialNumber>
      </Configuration>
    </FRU>
  </StdCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: FRU
  - XPath: `BmcCfg/StdCfg/FRU`
  - Sample XML Format:

```
<BmcCfg>
  <StdCfg Action="Change">
    <FRU Action="Change">
      <Configuration>
        <BoardMfgDateTime>1996/1/1 0:0</BoardMfgDateTime>
        <BoardMfgName></BoardMfgName>
        <BoardProductName></BoardProductName>
        <BoardSerialNum></BoardSerialNum>
        <BoardPartNum></BoardPartNum>
        <ProductMfgName></ProductMfgName>
        <ProductName></ProductName>
        <ProductPartModelNum></ProductPartModelNum>
        <ProductVersion></ProductVersion>
        <ProductSerialNum></ProductSerialNum>
        <ProductAssetTag></ProductAssetTag>
        <ChassisType>0x0</ChassisType>
        <ChassisPartNumber></ChassisPartNumber>
        <ChassisSerialNumber></ChassisSerialNumber>
      </Configuration>
    </FRU>
  </StdCfg>
</BmcCfg>
```

Q.1.1.13 Host Interface Management

The Host Interface configures the USB-based in-band network (RNDIS/CDC-ECM) between host OS and BMC.

- Table Type: In-Band
  - Table Name: HostInterface
  - XPath: `BmcCfg/OemCfg/HostInterface`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <HostInterface Action="Change">
      <Information>
        <HostIpAddress>169.254.3.1</HostIpAddress>
        <ServiceIpAddress>169.254.3.254</ServiceIpAddress>
      </Information>
      <Configuration>
        <HostInterfaceControl>Enable</HostInterfaceControl>
        <UsbConnection>RNDIS</UsbConnection>
      </Configuration>
    </HostInterface>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: HostInterface
  - XPath: `BmcCfg/OemCfg/HostInterface`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <HostInterface Action="Change">
      <Information>
        <ServiceIpAddress>169.254.3.254</ServiceIpAddress>
      </Information>
      <Configuration>
        <HostIpAddress>169.254.3.1</HostIpAddress>
        <HostInterfaceControl>Enable</HostInterfaceControl>
        <UsbConnection>RNDIS</UsbConnection>
      </Configuration>
    </HostInterface>
  </OemCfg>
</BmcCfg>
```

Q.1.1.14 IP Access Control Management

The IP Access Control creates whitelist/blacklist rules to permit or deny specific IP subnets reaching the BMC.

- Table Type: OOB
  - Table Name: IPAccessControl
  - XPath: `BmcCfg/OemCfg/IPAccessControl`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <IPAccessControl Action="Overwrite">
      <Information>
        <MaxAvailControlRule>10</MaxAvailControlRule>
        <CurrentAvailControlRule>0</CurrentAvailControlRule>
      </Information>
      <Configuration>
        <IPAccessControlStatus>Disable</IPAccessControlStatus>
        <ControlRule Action="Change" IPControlRuleNumber="0">
          <Configuration>
            <IPControlIPAddr></IPControlIPAddr>
            <IPControlPrefixLength>0</IPControlPrefixLength>
            <IPControlPolicy>Accept</IPControlPolicy>
          </Configuration>
        </ControlRule>
      </Configuration>
    </IPAccessControl>
  </OemCfg>
</BmcCfg>
```

Q.1.1.15 KCS Privilege Management

The KCS Privilege sets the minimum privilege level required for the local KCS/IPMI interface.

- Table Type: In-Band
  - Table Name: KCSPrivilege
  - XPath: `BmcCfg/OemCfg/KCSPrivilege`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <KCSPrivilege Action="Change">
      <Configuration>
        <PrivilegeLimit>Administrator</PrivilegeLimit>
      </Configuration>
    </KCSPrivilege>
```

```
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: KCSPrivilege
  - XPath: `BmcCfg/OemCfg/KCSPrivilege`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <KCSPrivilege Action="Change">
      <Configuration>
        <PrivilegeLimit>Administrator</PrivilegeLimit>
      </Configuration>
    </KCSPrivilege>
  </OemCfg>
</BmcCfg>
```

Q.1.1.16 LAN Management

The LAN configuration covers Ethernet mode (Dedicated/Shared/Failover), IP addressing, VLAN IDs, MAC and DNS options.

- Table Type: In-Band
  - Table Name: LAN
  - XPath: `BmcCfg/OemCfg/LAN`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <LAN Action="Change">
      <Configuration>
        <IPProtocolStatus>Dual</IPProtocolStatus>
        <LanMode>Failover</LanMode>
        <ShareLan>Auto</ShareLan>
        <MacAddr>XX:XX:XX:XX:XX:XX</MacAddr>
        <HostName></HostName>
        <CommunityString>public</CommunityString>
        <VLAN_Enable>Disable</VLAN_Enable>
        <VLAN_ID>1</VLAN_ID>
        <RMCP_Port>623</RMCP_Port>
        <IPv4 Action="Change">
          <Configuration>
            <IPSrc>DHCP</IPSrc>
            <IPAddr>192.168.34.56</IPAddr>
```

```
            <?Note Will be skipped in multiple system usage without --
individually option.?>
            <SubNetMask>255.255.0.0</SubNetMask>
            <?Note Will be skipped in multiple system usage without --
individually option.?>
            <DefaultGateWayAddr>192.168.34.1</DefaultGateWayAddr>
            <?Note Will be skipped in multiple system usage without --
individually option.?>
            <DNSv4Mode>Enable</DNSv4Mode>
            <DNSAddr>192.168.34.255</DNSAddr>
            <DNSAddr2>192.168.34.254</DNSAddr2>
          </Configuration>
        </IPv4>
        <DynamicIPv6 Action="Change">
          <Information>
            <TotalDynamicIPv6Group>3</TotalDynamicIPv6Group>
            <DUID>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</DUID>
            <IPv6DynamicGroup ID="1">
              <Address>X:X:X:X:X:X:X:X</Address>
              <PrefixLength>64</PrefixLength>
              <AddressOrigin>SLAAC</AddressOrigin>
            </IPv6DynamicGroup>
            <IPv6DynamicGroup ID="2">
              <Address>X:X:X:X:X:X:X:X</Address>
              <PrefixLength>64</PrefixLength>
              <AddressOrigin>SLAAC</AddressOrigin>
            </IPv6DynamicGroup>
            <IPv6DynamicGroup ID="3">
              <Address>X:X:X:X:X:X:X:X</Address>
              <PrefixLength>64</PrefixLength>
              <AddressOrigin>SLAAC</AddressOrigin>
            </IPv6DynamicGroup>
          </Information>
          <Configuration>
            <AutoConfiguration>Enable</AutoConfiguration>
            <DHCPv6Mode>Stateless</DHCPv6Mode>
          </Configuration>
        </DynamicIPv6>
        <StaticIPv6 Action="Change">
          <Information>
            <TotalStaticIPv6Group>0</TotalStaticIPv6Group>
          </Information>
          <Configuration>
            <DNSv6Mode>Disable</DNSv6Mode>
            <IPv6StaticNameServer></IPv6StaticNameServer>
            <IPv6StaticNameServer2></IPv6StaticNameServer2>
            <IPv6StaticGroup Action="Change" ID="1">
              <Configuration>
                <Address></Address>
                <PrefixLength>0</PrefixLength>
              </Configuration>
            </IPv6StaticGroup>
          </Configuration>
```

```
        </StaticIPv6>
      </Configuration>
    </LAN>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: LAN
  - XPath: `BmcCfg/OemCfg/LAN`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <LAN Action="Change">
      <Information>
        <MacAddress>XX:XX:XX:XX:XX:XX</MacAddress>
        <SpeedMbps>1000</SpeedMbps>
        <Duplex>Full Duplex</Duplex>
      </Information>
      <Configuration>
        <IPProtocolStatus>Dual</IPProtocolStatus>
        <LanInterface>Failover</LanInterface>
        <Link>Auto Negotiation</Link>
        <HostName></HostName>
        <?Note Will be skipped in multiple system usage without --
individually option.?>
        <VLANEnable>Disable</VLANEnable>
        <VLANId>1</VLANId>
        <RMCP_Port>623</RMCP_Port>
        <IPv4 Action="Change">
          <Information>
            <IPv4NameServer1>192.168.34.255</IPv4NameServer1>
            <IPv4NameServer2>192.168.34.254</IPv4NameServer2>
          </Information>
          <Configuration>
            <DHCPEnabled>Enable</DHCPEnabled>
            <Address>192.168.34.56</Address>
            <?Note Will be skipped in multiple system usage without --
individually option.?>
            <SubNetMask>255.255.0.0</SubNetMask>
            <?Note Will be skipped in multiple system usage without --
individually option.?>
            <Gateway>192.168.34.1</Gateway>
            <?Note Will be skipped in multiple system usage without --
individually option.?>
            <IPv4UseDNSServers>Enable</IPv4UseDNSServers>
            <IPv4StaticNameServer1></IPv4StaticNameServer1>
            <IPv4StaticNameServer2></IPv4StaticNameServer2>
          </Configuration>
        </IPv4>
        <IPv6 Action="Change">
```

```
          <Information>
            <IPv6LinkLocalAddress>X:X:X:X:X:X:X:X</IPv6LinkLocalAddress>

<IPv6LinkLocalAddressPrefixLength>64</IPv6LinkLocalAddressPrefixLength>
            <IPv6NameServer1></IPv6NameServer1>
            <IPv6NameServer2></IPv6NameServer2>
          </Information>
          <Configuration>
            <IPv6UseDNSServers>Disable</IPv6UseDNSServers>
            <DynamicIPv6 Action="Change">
              <Information>
                <TotalDynamicIPv6Group>3</TotalDynamicIPv6Group>
                <DUID></DUID>
                <IPv6DynamicGroup ID="1">
                  <Address>X:X:X:X:X:X:X:X</Address>
                  <PrefixLength>64</PrefixLength>
                  <AddressOrigin>SLAAC</AddressOrigin>
                </IPv6DynamicGroup>
                <IPv6DynamicGroup ID="2">
                  <Address>X:X:X:X:X:X:X:X</Address>
                  <PrefixLength>64</PrefixLength>
                  <AddressOrigin>SLAAC</AddressOrigin>
                </IPv6DynamicGroup>
                <IPv6DynamicGroup ID="3">
                  <Address>X:X:X:X:X:X:X:X</Address>
                  <PrefixLength>64</PrefixLength>
                  <AddressOrigin>SLAAC</AddressOrigin>
                </IPv6DynamicGroup>
              </Information>
              <Configuration>
                <IPv6AutoConfigEnabled>Enable</IPv6AutoConfigEnabled>
                <OperatingMode>Disabled</OperatingMode>
              </Configuration>
            </DynamicIPv6>
            <StaticIPv6 Action="Change">
              <Information>
                <TotalStaticIPv6Group>0</TotalStaticIPv6Group>
              </Information>
              <Configuration>
                <IPv6StaticNameServer1></IPv6StaticNameServer1>
                <IPv6StaticNameServer2></IPv6StaticNameServer2>
                <IPv6StaticDefaultGateway></IPv6StaticDefaultGateway>
                <?Note Will be skipped in multiple system usage without --
individually option.?>
                <IPv6StaticGroup Action="Change" ID="1">
                  <Configuration>
                    <?Note Will be skipped in multiple system usage
without --individually option.?>
                    <Address></Address>
                    <PrefixLength>64</PrefixLength>
                  </Configuration>
                </IPv6StaticGroup>
              </Configuration>
```

```
            </StaticIPv6>
          </Configuration>
        </IPv6>
      </Configuration>
    </LAN>
  </OemCfg>
</BmcCfg>
```

Q.1.1.17 Link Layer Discovery Protocol Management

The Link Layer Discovery Protocol (LLDP) settings control whether the BMC advertises itself on the network using Link Layer Discovery Protocol.

- Table Type: OOB
  - Table Name: LLDP
  - XPath: `BmcCfg/OemCfg/LLDP`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <LLDP Action="Change">
      <Information>
        <ChassisIdSubtype></ChassisIdSubtype>
        <ManagementAddressIPv4></ManagementAddressIPv4>
        <ManagementAddressIPv6></ManagementAddressIPv6>
        <ManagementAddressMAC></ManagementAddressMAC>
        <ManagementVlanId></ManagementVlanId>
        <ChassisId></ChassisId>
        <PortIdSubtype></PortIdSubtype>
        <PortId></PortId>
      </Information>
      <Configuration>
        <LLDPEnable>Disable</LLDPEnable>
      </Configuration>
    </LLDP>
  </OemCfg>
</BmcCfg>
```

Q.1.1.18 Power Supply Management

The Power Supply show total power capabilities, live consumption and allows SmartPower capping policies.

- Table Type: In-Band

- Table Name: PowerSupply
- XPath: `BmcCfg/OemCfg/PowerSupply`
- Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <PowerSupply Action="Change">
      <Information>
        <TotalPSUPower>2000</TotalPSUPower>
        <TotalMaxPower>0</TotalMaxPower>
        <TotalPowerConsumption>147</TotalPowerConsumption>
        <TotalPowerCapping>1940</TotalPowerCapping>
      </Information>
      <Configuration>
        <SmartPower>Enable</SmartPower>
      </Configuration>
    </PowerSupply>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: PowerSupply
  - XPath: `BmcCfg/OemCfg/PowerSupply`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <PowerSupply Action="Change">
      <Information>
        <TotalMaxPower>2000</TotalMaxPower>
        <TotalPowerConsumption>174</TotalPowerConsumption>
        <TotalPowerCapping>1940</TotalPowerCapping>
      </Information>
      <Configuration>
        <SmartPower>Enable</SmartPower>
      </Configuration>
    </PowerSupply>
  </OemCfg>
</BmcCfg>
```

Q.1.1.19 Redfish Session Management

The Redfish Session set the idle timeout for API sessions established via the Redfish interface.

- Table Type: OOB
  - Table Name: RedfishSession
  - XPath: `BmcCfg/OemCfg/RedfishSession`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <RedfishSession Action="Change">
      <Configuration>
        <RedfishSessionTimeout>1800</RedfishSessionTimeout>
      </Configuration>
    </RedfishSession>
  </OemCfg>
</BmcCfg>
```

Q.1.1.20 Service Enabling Management

The Service Enabling turn individual network services (HTTP, HTTPS, SSH, IKVM, SNMP, etc.) on or off.

- Table Type: In-Band
  - Table Name: ServiceEnabling
  - XPath: `BmcCfg/OemCfg/ServiceEnabling`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <ServiceEnabling Action="Change">
      <Configuration>
        <HTTP>Enable</HTTP>
        <HTTPS>Enable</HTTPS>
        <IKVM>Enable</IKVM>
        <VirtualMedia>Enable</VirtualMedia>
        <SSH>Enable</SSH>
        <SSL_Redirect>Enable</SSL_Redirect>
        <SNMP>Disable</SNMP>
      </Configuration>
    </ServiceEnabling>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: ServiceEnabling

- XPath: `BmcCfg/OemCfg/ServiceEnabling`
- Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <ServiceEnabling Action="Change">
      <Configuration>
        <HTTP>Enable</HTTP>
        <HTTPS>Enable</HTTPS>
        <IKVM>Enable</IKVM>
        <VirtualMedia>Enable</VirtualMedia>
        <SSH>Enable</SSH>
        <SSL_Redirect>Enable</SSL_Redirect>
        <SNMP>Disable</SNMP>
      </Configuration>
    </ServiceEnabling>
  </OemCfg>
</BmcCfg>
```

Q.1.1.21 Service Port Management

The Service Port allows administrators change the listening ports used by the BMC's network services.

- Table Type: In-Band
  - Table Name: ServicePort
  - XPath: `BmcCfg/OemCfg/ServicePort`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <ServicePort Action="Change">
      <Configuration>
        <HTTP>80</HTTP>
        <HTTPS>443</HTTPS>
        <IKVM>5900</IKVM>
        <VirtualMedia>623</VirtualMedia>
        <SSH>22</SSH>
        <SNMP>161</SNMP>
      </Configuration>
    </ServicePort>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB

- Table Name: ServicePort
- XPath: `BmcCfg/OemCfg/ServicePort`
- Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <ServicePort Action="Change">
      <Configuration>
        <HTTP>80</HTTP>
        <HTTPS>443</HTTPS>
        <IKVM>5900</IKVM>
        <VirtualMedia>623</VirtualMedia>
        <SSH>22</SSH>
        <SNMP>161</SNMP>
      </Configuration>
    </ServicePort>
  </OemCfg>
</BmcCfg>
```

Q.1.1.22 RAKP Management

The Remote Authenticated Key-Exchange Protocol (RAKP) toggles Supermicro's proprietary RAKP mechanism, affecting IPMI authentication behavior and related vulnerabilities.

- Table Type: OOB
  - Table Name: SMCRAKP
  - XPath: `BmcCfg/OemCfg/SMCRAKP`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <SMCRAKP Action="Change">
      <Configuration>
        <RAKPEnable>Disable</RAKPEnable>
      </Configuration>
    </SMCRAKP>
  </OemCfg>
</BmcCfg>
```

Q.1.1.23 SMTP Management

The SMTP defines the mail server, credentials and port the BMC uses to send e-mail alerts.

- Table Type: In-Band
  - Table Name: SMTP
  - XPath: `BmcCfg/OemCfg/SMTP`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <SMTP Action="Change">
      <Configuration>
        <SSLAuthentication>Disable</SSLAuthentication>
        <ServerURL>0.0.0.0</ServerURL>
        <ServerPort>587</ServerPort>
        <UserName></UserName>
        <UserPassword></UserPassword>
        <SenderEmail></SenderEmail>
      </Configuration>
    </SMTP>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: SMTP
  - XPath: `BmcCfg/OemCfg/SMTP`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <SMTP Action="Change">
      <Configuration>
        <ServerAddress>0.0.0.0</ServerAddress>
        <Port>587</Port>
        <ConnectionProtocol>None</ConnectionProtocol>
        <Authentication>None</Authentication>
        <UserName></UserName>
        <Password></Password>
        <FromAddress></FromAddress>
      </Configuration>
    </SMTP>
  </OemCfg>
</BmcCfg>
```

Q.1.1.24 SNMP Management

SNMP enables SNMP v2/v3, defines community strings and sets authentication/encryption options for monitoring tools.

- Table Type: OOB
  - Table Name: SNMP
  - XPath: `BmcCfg/OemCfg/SNMP`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <SNMP Action="Change">
      <Configuration>
        <SNMPV2 Action="Change">
          <EnableSNMPv2c>Disable</EnableSNMPv2c>
          <HideCommunityStrings>Disable</HideCommunityStrings>
          <CommunityStrings Action="Change" CommunityStringID="0">
            <Configuration>
              <AccessMode>ReadOnly</AccessMode>
              <Name></Name>
              <CommunityString></CommunityString>
            </Configuration>
          </CommunityStrings>
        </SNMPV2>
        <SNMPV3 Action="Change">
          <EnableSNMPv3>Disable</EnableSNMPv3>
          <AuthenticationProtocol>HMAC_MD5</AuthenticationProtocol>
          <EncryptionProtocol>CBC_DES</EncryptionProtocol>
        </SNMPV3>
      </Configuration>
    </SNMP>
  </OemCfg>
</BmcCfg>
```

Q.1.1.25 SOL Management

The Serial-over-LAN (SOL) provides a remote text console by redirecting the system's serial port over IP.

- Table Type: In-Band
  - Table Name: SOL
  - XPath: `BmcCfg/StdCfg/SOL`
  - Sample XML Format:

```
<BmcCfg>
  <StdCfg Action="Change">
    <SOL Action="Change">
      <Configuration>
        <Access>Enable</Access>
        <PrivilegeLimit>Operator</PrivilegeLimit>
        <BitRate>115200</BitRate>
        <CharAccTime>0</CharAccTime>
        <CharAccSize>0</CharAccSize>
        <RetryLimit>0</RetryLimit>
        <RetryTime>0</RetryTime>
      </Configuration>
    </SOL>
  </StdCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: SOL
  - XPath: `BmcCfg/StdCfg/SOL`
  - Sample XML Format:

```
<BmcCfg>
  <StdCfg Action="Change">
    <SOL Action="Change">
      <Configuration>
        <Access>Enable</Access>
        <PrivilegeLimit>Operator</PrivilegeLimit>
        <BitRate>115200</BitRate>
        <CharAccTime>0</CharAccTime>
        <CharAccSize>0</CharAccSize>
        <RetryLimit>0</RetryLimit>
        <RetryTime>0</RetryTime>
      </Configuration>
    </SOL>
  </StdCfg>
</BmcCfg>
```

Q.1.1.26 SSDP Management

The SSDP broadcast allows the BMC to announce its presence via Simple Service Discovery Protocol on the local network.

- Table Type: OOB
  - Table Name: SSDP
  - XPath: `BmcCfg/OemCfg/SSDP`

- Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <SSDP Action="Change">
      <Configuration>
        <SSDPEnable>Enable</SSDPEnable>
        <Port>1900</Port>
        <NotifyTTL>2</NotifyTTL>
        <NotifyIPv6Scope>Link</NotifyIPv6Scope>
      </Configuration>
    </SSDP>
  </OemCfg>
</BmcCfg>
```

Q.1.1.27 Syslog Management

The Syslog forwarding sends BMC event messages to an external syslog server for centralized logging.

- Table Type: OOB
  - Table Name: Syslog
  - XPath: `BmcCfg/OemCfg/Syslog`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <Syslog Action="Change">
      <Configuration>
        <SyslogEnable>Disable</SyslogEnable>
        <SyslogServerIP></SyslogServerIP>
        <SyslogPortNumber>514</SyslogPortNumber>
      </Configuration>
    </Syslog>
  </OemCfg>
</BmcCfg>
```

Q.1.1.28 UI Control Management

The UI Control changes the mouse-tracking mode (Absolute/Relative/Single) used in the KVM console.

- Table Type: In-Band
  - Table Name: UIControl

- XPath: `BmcCfg/OemCfg/UIControl`
- Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <UIControl Action="Change">
      <Configuration>
        <MouseMode>Absolute</MouseMode>
      </Configuration>
    </UIControl>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: UIControl
  - XPath: `BmcCfg/OemCfg/UIControl`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <UIControl Action="Change">
      <Configuration>
        <MouseMode>Absolute</MouseMode>
      </Configuration>
    </UIControl>
  </OemCfg>
</BmcCfg>
```

Q.1.1.29 Virtual Media Management

The Virtual Media mounts remote ISO, USB or floppy images so the host can boot or access them as local devices via IKVM.

- Table Type: In-Band
  - Table Name: VirtualMedia
  - XPath: `BmcCfg/OemCfg/VirtualMedia`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <VirtualMedia Action="Change">
      <Information>
        <DeviceStatus>Unmounted</DeviceStatus>
      </Information>
```

```
      <Configuration>
        <ShareHost></ShareHost>
        <PathToImage></PathToImage>
        <UserName></UserName>
        <UserPassword></UserPassword>
      </Configuration>
    </VirtualMedia>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: VirtualMedia
  - XPath: `BmcCfg/OemCfg/VirtualMedia`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <VirtualMedia Action="Change">
      <Information>
        <MaximumAvailableDevNums>3</MaximumAvailableDevNums>
      </Information>
      <Configuration>
        <VMDevice Action="Change" DeviceNumber="1">
          <Information>
            <MediaType></MediaType>
          </Information>
          <Configuration>
            <ShareHost></ShareHost>
            <PathToImage></PathToImage>
            <UserName></UserName>
            <UserPassword></UserPassword>
            <VerifyCert>Disable</VerifyCert>
            <AcceptSelfSigned>Disable</AcceptSelfSigned>
            <Inserted>Disable</Inserted>
          </Configuration>
        </VMDevice>
        <VMDevice Action="Change" DeviceNumber="2">
          <Information>
            <MediaType></MediaType>
          </Information>
          <Configuration>
            <ShareHost></ShareHost>
            <PathToImage></PathToImage>
            <UserName></UserName>
            <UserPassword></UserPassword>
            <VerifyCert>Disable</VerifyCert>
            <AcceptSelfSigned>Disable</AcceptSelfSigned>
            <Inserted>Disable</Inserted>
          </Configuration>
        </VMDevice>
        <VMDevice Action="Change" DeviceNumber="3">
```

```
            <Information>
              <MediaType></MediaType>
            </Information>
            <Configuration>
              <ShareHost></ShareHost>
              <PathToImage></PathToImage>
              <UserName></UserName>
              <UserPassword></UserPassword>
              <VerifyCert>Disable</VerifyCert>
              <AcceptSelfSigned>Disable</AcceptSelfSigned>
              <Inserted>Disable</Inserted>
            </Configuration>
          </VMDevice>
        </Configuration>
      </VirtualMedia>
    </OemCfg>
</BmcCfg>
```

Q.1.1.30 Web Session Management

The Web Session sets the inactivity timeout for browser-based BMC sessions to enhance security.

- Table Type: In-Band
  - Table Name: WebSession
  - XPath: `BmcCfg/OemCfg/WebSession`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <WebSession Action="Change">
      <Configuration>
        <Timeout>30</Timeout>
      </Configuration>
    </WebSession>
  </OemCfg>
</BmcCfg>
```

- Table Type: OOB
  - Table Name: WebSession
  - XPath: `BmcCfg/OemCfg/WebSession`
  - Sample XML Format:

```
<BmcCfg>
  <OemCfg Action="Change">
    <WebSession Action="Change">
      <Configuration>
        <Timeout>30</Timeout>
      </Configuration>
    </WebSession>
  </OemCfg>
</BmcCfg>
```

Q.1.2 Sample CMM Configuration Table

The sample CMM configuration tables below are from CMM6.

Q.1.2.1 Account Management

Account Management controls local CMM users, passwords, privileges and lock-out policies.

- Table Type: OOB
  - Table Name: Account
  - XPath: `CmmCfg/OemCfg/Account`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <Account Action="Change">
      <Information>
        <MaximumAvailableIDs>16</MaximumAvailableIDs>
        <TotalIDEnabled>1</TotalIDEnabled>
      </Information>
      <Configuration>
        <AccountLockoutThreshold>0</AccountLockoutThreshold>

<AccountLockoutCounterResetAfter>0</AccountLockoutCounterResetAfter>
        <AccountLockoutDuration>0</AccountLockoutDuration>
        <User Action="Change" UserID="2">
          <Configuration>
            <UserName><![CDATA[ADMIN]]></UserName>
            <Password><![CDATA[]]></Password>
            <RoleId>Administrator</RoleId>
            <Locked>false</Locked>
            <Enabled>Enable</Enabled>
          </Configuration>
        </User>
      </Configuration>
```

```
    </Account>
  </OemCfg>
</CmmCfg>
```

Q.1.2.2 AD Management

Active Directory (AD) allows CMM web logins to be authenticated against Microsoft AD domains.

- Table Type: OOB
  - Table Name: AD
  - XPath: `CmmCfg/OemCfg/AD`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <AD Action="Overwrite">
      <Information>
        <MaximumAvailableADGroup>5</MaximumAvailableADGroup>
        <TotalConfiguredADGroup>0</TotalConfiguredADGroup>
        <DynamicServerAddress1></DynamicServerAddress1>
        <DynamicServerAddress2></DynamicServerAddress2>
        <DynamicServerAddress3></DynamicServerAddress3>
        <DynamicServerAddress4></DynamicServerAddress4>
        <DynamicServerAddress5></DynamicServerAddress5>
      </Information>
      <Configuration>
        <ADEnable>Disable</ADEnable>
        <DNSLookupEnable>Disable</DNSLookupEnable>
        <Prefix>ldaps</Prefix>
        <Port>389</Port>
        <UserDomainName1></UserDomainName1>
        <UserDomainName2></UserDomainName2>
        <UserDomainName3></UserDomainName3>
        <UserDomainName4></UserDomainName4>
        <UserDomainName5></UserDomainName5>
        <ServiceAddr1></ServiceAddr1>
        <ServiceAddr2></ServiceAddr2>
        <ServiceAddr3></ServiceAddr3>
        <ADRule Action="Change" RuleID="1">
          <Configuration>
            <RemoteUser><![CDATA[]]></RemoteUser>
            <RemoteGroup><![CDATA[]]></RemoteGroup>
            <RulePrivilege>None</RulePrivilege>
          </Configuration>
        </ADRule>
      </Configuration>
    </AD>
```

```
  </OemCfg>
</CmmCfg>
```

Q.1.2.3 LDAP Management

LDAP integration enables authentication of CMM logins against an external LDAP directory service.

- Table Type: OOB
  - Table Name: LDAP
  - XPath: `CmmCfg/OemCfg/LDAP`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <LDAP Action="Overwrite">
      <Information>
        <MaximumAvailableADGroup>5</MaximumAvailableADGroup>
        <TotalConfiguredADGroup>0</TotalConfiguredADGroup>
      </Information>
      <Configuration>
        <LDAPEnable>Disable</LDAPEnable>
        <BindDN></BindDN>
        <BindPassword></BindPassword>
        <UsernameAttribute></UsernameAttribute>
        <GroupsAttribute></GroupsAttribute>
        <SearchBase1></SearchBase1>
        <SearchBase2></SearchBase2>
        <SearchBase3></SearchBase3>
        <ServiceAddr1></ServiceAddr1>
        <ServiceAddr2></ServiceAddr2>
        <ServiceAddr3></ServiceAddr3>
        <LDAPRule Action="Change" RuleID="1">
          <Configuration>
            <RemoteUser><![CDATA[]]></RemoteUser>
            <RemoteGroup><![CDATA[]]></RemoteGroup>
            <RulePrivilege>None</RulePrivilege>
          </Configuration>
        </LDAPRule>
      </Configuration>
    </LDAP>
  </OemCfg>
</CmmCfg>
```

Q.1.2.4 RADIUS Management

RADIUS authentication allows the CMM to validate user credentials through an external RADIUS server.

- Table Type: OOB
  - Table Name: RADIUS
  - XPath: `CmmCfg/OemCfg/RADIUS`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <RADIUS Action="Change">
      <Configuration>
        <RADIUSEnable>Disable</RADIUSEnable>
        <Port>1812</Port>
        <ServerAddress>0.0.0.0</ServerAddress>
        <Secret></Secret>
      </Configuration>
    </RADIUS>
  </OemCfg>
</CmmCfg>
```

Q.1.2.5 Advance Event Log Management

Advanced Event Log records additional system events such as AC-power-on for detailed auditing.

- Table Type: OOB
  - Table Name: AdvanceEventLog
  - XPath: `CmmCfg/OemCfg/AdvanceEventLog`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <AdvanceEventLog Action="Change">
      <Configuration>
        <ACPowerOnEventLog>Enable</ACPowerOnEventLog>
      </Configuration>
    </AdvanceEventLog>
  </OemCfg>
</CmmCfg>
```

Q.1.2.6 Alert Management

Alert List configures up to 16 alert destinations and protocols (SNMP, SMTP, Redfish) for event notification.

- Table Type: OOB
  - Table Name: AlertList
  - XPath: `CmmCfg/OemCfg/AlertList`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <AlertList Action="Change">
      <Information>
        <MaximumAvailableAlerts>16</MaximumAvailableAlerts>
        <TotalConfiguredAlerts>1</TotalConfiguredAlerts>
      </Information>
      <Configuration>
        <Alert Action="Change" AlertNumber="1">
          <Configuration>
            <Enable>Enable</Enable>
            <Protocol>SNMPv1</Protocol>
            <EventType></EventType>
            <Destination>0.0.0.0</Destination>
            <Severity>Information</Severity>
            <TrapCommunity></TrapCommunity>
            <MailMessage></MailMessage>
            <MailSubject></MailSubject>
            <UserName></UserName>
            <AuthenticationKey></AuthenticationKey>
            <AuthenticationProtocol>HMAC_MD5</AuthenticationProtocol>
            <EncryptionKey></EncryptionKey>
            <EncryptionProtocol>CBC_DES</EncryptionProtocol>
          </Configuration>
        </Alert>
      </Configuration>
    </AlertList>
  </OemCfg>
</CmmCfg>
```

Q.1.2.7 Blade Management

Blade Management configures blade IP schemes, node power policies and names across the enclosure.

- Table Type: OOB
  - Table Name: BladeManage

- XPath: `CmmCfg/OemCfg/BladeManage`
- Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <BladeManage Action="Change">
      <Information>
        <Count>2</Count>
      </Information>
      <Configuration>
        <BladeNetwork Action="Change">
          <IPSrc>DHCP</IPSrc>
          <IPScale>4</IPScale>
          <BaseIPAddress>0.0.0.0</BaseIPAddress>
          <SubnetMask>0.0.0.0</SubnetMask>
          <Gateway>0.0.0.0</Gateway>
          <DNSServerIP>0.0.0.0</DNSServerIP>
          <VLAN_ID>0</VLAN_ID>
          <BladeNetworkPolicy>One Time</BladeNetworkPolicy>
        </BladeNetwork>
        <Blade Action="Change" BladeID="A1">
          <Information>
            <Count>1</Count>
          </Information>
          <Configuration>
            <Node Action="Change" ID="1">
              <PowerFailPolicy>Throttle</PowerFailPolicy>
              <ACLostPolicy>LastState</ACLostPolicy>
              <PowerCapping>ReadOnly</PowerCapping>
              <Name></Name>
              <IPMIHostName>testlan</IPMIHostName>
            </Node>
          </Configuration>
        </Blade>
        <Blade Action="Change" BladeID="A7">
          <Information>
            <Count>1</Count>
          </Information>
          <Configuration>
            <Node Action="Change" ID="1">
              <PowerFailPolicy>Throttle</PowerFailPolicy>
              <ACLostPolicy>LastState</ACLostPolicy>
              <PowerCapping>ReadOnly</PowerCapping>
              <Name></Name>
              <IPMIHostName>ATTBMCCfgLANTest</IPMIHostName>
            </Node>
          </Configuration>
        </Blade>
      </Configuration>
    </BladeManage>
```

```
  </OemCfg>
</CmmCfg>
```

Q.1.2.8 LAN Management

LAN configuration covers Ethernet mode (Dedicated/Shared/Failover), IP addressing, VLAN IDs, MAC and DNS options.

- Table Type: OOB
  - Table Name: CMMLAN
  - XPath: `CmmCfg/OemCfg/CMMLAN`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <CMMLAN Action="Change">
      <Information>
        <MacAddr>XX:XX:XX:XX:XX:XX</MacAddr>
      </Information>
      <Configuration>
        <LanMode>Dedicated</LanMode>
        <HostName></HostName>
        <?Note Will be skipped in multiple system usage without --
individually option.?>
        <IPSrc>FailOver</IPSrc>
        <IPAddr>192.168.34.56</IPAddr>
        <?Note Will be skipped in multiple system usage without --
individually option.?>
        <SubNetMask>255.255.0.0</SubNetMask>
        <DefaultGateWayAddr>192.168.34.1</DefaultGateWayAddr>
        <DNSAddr>192.168.34.255</DNSAddr>
        <DNSAddr2>192.168.34.254</DNSAddr2>
        <CommunityString>test</CommunityString>
        <VLAN_Enable>Disable</VLAN_Enable>
        <VLAN_ID>0</VLAN_ID>
        <RMCP_Port>623</RMCP_Port>
      </Configuration>
    </CMMLAN>
  </OemCfg>
</CmmCfg>
```

Q.1.2.9 Certification Management

Certificate Management lets administrators upload custom SSL certificates and private keys for HTTPS/Redfish.

- Table Type: OOB
  - Table Name: Certification
  - XPath: `CmmCfg/OemCfg/Certification`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <Certification Action="Change">
      <Information>
        <CertStartDate>Mar 20 00:00:00 2025 GMT</CertStartDate>
        <CertEndDate>Mar 20 00:00:00 2028 GMT</CertEndDate>
      </Information>
      <Configuration>
        <CertFile></CertFile>
        <PrivKeyFile></PrivKeyFile>
      </Configuration>
    </Certification>
  </OemCfg>
</CmmCfg>
```

Q.1.2.10 CMM Identification Management

CMM Identification stores location fields such as data-center, rack or chassis names for inventory tracking.

- Table Type: OOB
  - Table Name: CMM
  - XPath: `CmmCfg/OemCfg/CMM`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <CMM Action="Change">
      <Information>
        <FirmwareVersion>09.75.20</FirmwareVersion>
      </Information>
      <Configuration>
        <DataCenterName></DataCenterName>
        <RoomName></RoomName>
        <AisleName></AisleName>
        <RackName></RackName>
        <RackSlot></RackSlot>
        <ChassisLocation></ChassisLocation>
        <Name></Name>
      </Configuration>
```

```
    </CMM>
  </OemCfg>
</CmmCfg>
```

Q.1.2.11 DateTime Management

Date & Time sets the CMM clock, timezone, daylight-saving and optional NTP servers.

- Table Type: OOB
  - Table Name: DateTime
  - XPath: `CmmCfg/OemCfg/DateTime`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <DateTime Action="Change">
      <Information>
        <DateTimeValue>1970/4/21 3:57:8</DateTimeValue>
      </Information>
      <Configuration>
        <TimeUpdateMode>Local</TimeUpdateMode>
        <NTPPrimaryServer>localhost</NTPPrimaryServer>
        <NTPSecondaryServer>127.0.0.1</NTPSecondaryServer>
        <TimeZone>(UTC+00:00) Coordinated Universal Time</TimeZone>
        <AutoDSTEnabled>Disable</AutoDSTEnabled>
      </Configuration>
    </DateTime>
  </OemCfg>
</CmmCfg>
```

Q.1.2.12 Device Control Management

Device Control adjusts hardware behavior such as the system-wide fan mode (Standard, Full, Optimal).

- Table Type: OOB
  - Table Name: DeviceControl
  - XPath: `CmmCfg/OemCfg/DeviceControl`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <DeviceControl Action="Change">
```

```
      <Configuration>
        <FanMode>Standard</FanMode>
      </Configuration>
    </DeviceControl>
  </OemCfg>
</CmmCfg>
```

Q.1.2.13 DDNS Management

Dynamic DNS (DDNS) allows the CMM to register its hostname automatically when its IP address changes.

- Table Type: OOB
  - Table Name: DDNS
  - XPath: `CmmCfg/OemCfg/DDNS`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <DDNS Action="Change">
      <Configuration>
        <DDNSEnable>Disable</DDNSEnable>
        <TSIGEnable>Disable</TSIGEnable>
        <ServerIP>0.0.0.0</ServerIP>
        <CmmHostName></CmmHostName>
        <?Note Will be skipped in multiple system usage without --
individually option.?>
        <TSIGPubKeyFile></TSIGPubKeyFile>
        <TSIGPrivKeyFile></TSIGPrivKeyFile>
      </Configuration>
    </DDNS>
  </OemCfg>
</CmmCfg>
```

Q.1.2.14 FRU Management

Field Replaceable Unit (FRU) stores manufacturing, serial-number and part information for board, chassis and product identification.

- Table Type: OOB
  - Table Name: FRU
  - XPath: `CmmCfg/StdCfg/FRU`

- Sample XML Format:

```
<CmmCfg>
  <StdCfg Action="Change">
    <FRU>
      <Information>
        <BoardMfgDateTime>2023/1/5 17:15</BoardMfgDateTime>
        <BoardMfgName>Supermicro</BoardMfgName>
        <BoardProductName></BoardProductName>
        <BoardSerialNum></BoardSerialNum>
        <BoardPartNum>MBB-CMM-6</BoardPartNum>
        <ProductMfgName>Supermicro</ProductMfgName>
        <ProductName>Chassis Management Module</ProductName>
        <ProductPartModelNum>MBM-CMM-6</ProductPartModelNum>
        <ProductVersion></ProductVersion>
        <ProductSerialNum></ProductSerialNum>
        <ProductAssetTag></ProductAssetTag>
        <ChassisType>0x0</ChassisType>
        <ChassisPartNumber></ChassisPartNumber>
        <ChassisSerialNumber></ChassisSerialNumber>
      </Information>
    </FRU>
  </StdCfg>
</CmmCfg>
```

Q.1.2.15 IP Access Control Management

IP Access Control creates whitelist/blacklist rules to permit or deny specific IP subnets reaching the CMM.

- Table Type: OOB
  - Table Name: IPAccessControl
  - XPath: `CmmCfg/OemCfg/IPAccessControl`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <IPAccessControl Action="Overwrite">
      <Information>
        <MaxAvailControlRule>10</MaxAvailControlRule>
        <CurrentAvailControlRule>0</CurrentAvailControlRule>
      </Information>
      <Configuration>
        <IPAccessControlStatus>Disable</IPAccessControlStatus>
        <ControlRule Action="Change" IPControlRuleNumber="0">
          <Configuration>
            <IPControlIPAddr></IPControlIPAddr>
```

```
            <IPControlPrefixLength>0</IPControlPrefixLength>
            <IPControlPolicy>Accept</IPControlPolicy>
          </Configuration>
        </ControlRule>
      </Configuration>
    </IPAccessControl>
  </OemCfg>
</CmmCfg>
```

Q.1.2.16 Power Supply Management

Power Supply displays the number of PSUs and sets redundancy or smart-power policies.

- Table Type: OOB
  - Table Name: PowerSupply
  - XPath: `CmmCfg/OemCfg/PowerSupply`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <PowerSupply Action="Change">
      <Information>
        <Count>8</Count>
      </Information>
      <Configuration>
        <RedundancyPolicy>Max Power</RedundancyPolicy>
        <SmartPowerControl>Disable</SmartPowerControl>
        <ControlPolicy>Auto Control</ControlPolicy>
        <SettingFanSpeedLevel>5</SettingFanSpeedLevel>
      </Configuration>
    </PowerSupply>
  </OemCfg>
</CmmCfg>
```

Q.1.2.17 Redfish Session Management

Redfish Session sets the idle timeout for API sessions established via the Redfish interface.

- Table Type: OOB
  - Table Name: RedfishSession
  - XPath: `CmmCfg/OemCfg/RedfishSession`

- Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <RedfishSession Action="Change">
      <Configuration>
        <SessionTimeout>1800</SessionTimeout>
      </Configuration>
    </RedfishSession>
  </OemCfg>
</CmmCfg>
```

Q.1.2.18 Service Enabling Management

Service Enabling settings turn individual CMM network services such as HTTP, HTTPS, SSH or SNMP on or off.

- Table Type: OOB
  - Table Name: ServiceEnabling
  - XPath: `CmmCfg/OemCfg/ServiceEnabling`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <ServiceEnabling Action="Change">
      <Configuration>
        <HTTP>Enable</HTTP>
        <HTTPS>Enable</HTTPS>
        <SSH>Enable</SSH>
        <WS_Management>Disable</WS_Management>
        <SSL_Redirect>Enable</SSL_Redirect>
        <SNMP>Disable</SNMP>
      </Configuration>
    </ServiceEnabling>
  </OemCfg>
</CmmCfg>
```

Q.1.2.19 Service Port Management

Service Port lets administrators change the listening ports used by the CMM's network services.

- Table Type: OOB
  - Table Name: ServicePort

- XPath: `CmmCfg/OemCfg/ServicePort`
- Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <ServicePort Action="Change">
      <Configuration>
        <HTTP>80</HTTP>
        <HTTPS>443</HTTPS>
        <SSH>22</SSH>
        <WS_Management>5985</WS_Management>
        <SNMP>161</SNMP>
      </Configuration>
    </ServicePort>
  </OemCfg>
</CmmCfg>
```

Q.1.2.20 RAKP Management

Remote Authenticated Key-Exchange Protocol (RAKP) toggles Supermicro's proprietary RAKP mechanism, affecting IPMI authentication behavior and related vulnerabilities.

- Table Type: OOB
  - Table Name: SMCRAKP
  - XPath: `CmmCfg/OemCfg/SMCRAKP`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <SMCRAKP Action="Change">
      <Configuration>
        <RAKPEnable>Disable</RAKPEnable>
      </Configuration>
    </SMCRAKP>
  </OemCfg>
</CmmCfg>
```

Q.1.2.21 SMTP Management

SMTP defines the mail server, credentials and port the CMM uses to send e-mail alerts.

- Table Type: OOB

- Table Name: SMTP
- XPath: `CmmCfg/OemCfg/SMTP`
- Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <SMTP Action="Change">
      <Configuration>
        <SSLAuthentication>Disable</SSLAuthentication>
        <ServerURL></ServerURL>
        <ServerPort>587</ServerPort>
        <UserName></UserName>
        <UserPassword></UserPassword>
        <SenderEmail></SenderEmail>
      </Configuration>
    </SMTP>
  </OemCfg>
</CmmCfg>
```

Q.1.2.22 SNMP Management

The SNMP enables SNMP v2/v3, defines community strings and sets authentication/encryption options for monitoring tools.

- Table Type: OOB
  - Table Name: SNMP
  - XPath: `CmmCfg/OemCfg/SNMP`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <SNMP Action="Change">
      <Configuration>
        <SNMPV2 Action="Change">
          <EnableSNMPv2c>Disable</EnableSNMPv2c>
          <HideCommunityStrings>Disable</HideCommunityStrings>
          <CommunityStrings Action="Change" CommunityStringID="0">
            <Configuration>
              <AccessMode>ReadOnly</AccessMode>
              <Name></Name>
              <CommunityString></CommunityString>
            </Configuration>
          </CommunityStrings>
        </SNMPV2>
        <SNMPV3 Action="Change">
          <EnableSNMPv3>Disable</EnableSNMPv3>
```

```
            <AuthenticationProtocol>HMAC_MD5</AuthenticationProtocol>
            <EncryptionProtocol>CBC_DES</EncryptionProtocol>
          </SNMPV3>
        </Configuration>
      </SNMP>
    </OemCfg>
  </CmmCfg>
```

Q.1.2.23 SOL Management

The Serial-over-LAN (SOL) provides a remote text console by redirecting the system's serial port over IP.

- Table Type: OOB
  - Table Name: SOL
  - XPath: `CmmCfg/StdCfg/SOL`
  - Sample XML Format:

```
<CmmCfg>
  <StdCfg Action="Change">
    <SOL Action="Change">
      <Configuration>
        <Access>Enable</Access>
        <PrivilegeLimit>Operator</PrivilegeLimit>
        <BitRate>115200</BitRate>
        <CharAccTime>0</CharAccTime>
        <CharAccSize>0</CharAccSize>
        <RetryLimit>0</RetryLimit>
        <RetryTime>0</RetryTime>
      </Configuration>
    </SOL>
  </StdCfg>
</CmmCfg>
```

Q.1.2.24 SSDP Management

The SSDP broadcast allows the CMM to announce its presence via Simple Service Discovery Protocol on the local network.

- Table Type: OOB
  - Table Name: SSDP
  - XPath: `CmmCfg/OemCfg/SSDP`

- Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <SSDP Action="Change">
      <Configuration>
        <SSDPEnable>Enable</SSDPEnable>
        <Port>1900</Port>
        <NotifyMulticastIntervalSeconds>0</NotifyMulticastIntervalSeconds>
        <NotifyTTL>2</NotifyTTL>
        <NotifyIPv6Scope>Link</NotifyIPv6Scope>
      </Configuration>
    </SSDP>
  </OemCfg>
</CmmCfg>
```

Q.1.2.25 Switch Management

The Switch List manages credentials, date/time source, and IP settings for each installed switch module.

- Table Type: OOB
  - Table Name: SwitchList
  - XPath: `CmmCfg/OemCfg/SwitchList`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <SwitchList Action="Change">
      <Information>
        <Count>1</Count>
      </Information>
      <Configuration>
        <Switch Action="Change" DevId="A1">
          <SwitchUser Action="None">
            <User Action="Change">
              <UserName><![CDATA[ADMIN]]></UserName>
              <Password><![CDATA[]]></Password>
              <Privilege>ADMIN</Privilege>
            </User>
          </SwitchUser>
          <DateTime Action="Change">
            <DateTimeMode>Local</DateTimeMode>
          </DateTime>
          <Network Action="Change">
            <IPSrc>DHCP</IPSrc>
            <IPAddress>192.168.34.58</IPAddress>
```

```
            <?Note Will be skipped in multiple system usage without --
individually option.?>
            <Subnetmask>255.255.0.0</Subnetmask>
            <Gateway>192.168.34.1</Gateway>
          </Network>
        </Switch>
      </Configuration>
    </SwitchList>
  </OemCfg>
</CmmCfg>
```

Q.1.2.26 Syslog Management

The Syslog forwarding sends CMM event messages to an external syslog server for centralised logging.

- Table Type: OOB
  - Table Name: Syslog
  - XPath: `CmmCfg/OemCfg/Syslog`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <Syslog Action="Change">
      <Configuration>
        <SyslogEnable>Disable</SyslogEnable>
        <SyslogServerIP>0.0.0.0</SyslogServerIP>
        <SyslogPortNumber>514</SyslogPortNumber>
      </Configuration>
    </Syslog>
  </OemCfg>
</CmmCfg>
```

Q.1.2.27 Web Session Management

The Web Session sets the inactivity timeout for browser-based CMM sessions to enhance security.

- Table Type: OOB
  - Table Name: WebSession
  - XPath: `CmmCfg/OemCfg/WebSession`
  - Sample XML Format:

```
<CmmCfg>
  <OemCfg Action="Change">
    <WebSession Action="Change">
      <Configuration>
        <Timeout>30</Timeout>
      </Configuration>
    </WebSession>
  </OemCfg>
</CmmCfg>
```

Q.1.3 NVIDIA BMC Configuration Tables (Examples)

The NVIDIA BMC configuration tables below are from NVIDIA GB200 System.

Q.1.3.1 Account Management

The Account Management controls local BMC users, passwords and privileges.

- Table Type: OOB
  - Table Name: Account
  - XPath: `BmcCfg/NvidiaCfg/Account`
  - Sample XML Format:

```
<BmcCfg>
  <NvidiaCfg Action="Change">
    <Account Action="Change">
      <Information>
        <RolePrivileges>
          <Role ID="Administrator">
            <Privileges>
              Configure components managed by this service,
              Configure manager resources,
              Update password for current user account,
              Configure users and their accounts,
              Log in to the service and read resources
            </Privileges>
          </Role>
          <Role ID="Operator">
            <Privileges>
              Configure components managed by this service,
              Update password for current user account,
              Log in to the service and read resources
            </Privileges>
          </Role>
          <Role ID="ReadOnly">
            <Privileges>
```

```
              Update password for current user account,
              Log in to the service and read resources
            </Privileges>
          </Role>
          <Role ID="NoAccess">
            <Privileges>
              No privileges assigned
            </Privileges>
          </Role>
        </RolePrivileges>
      </Information>
      <Configuration>
        <AccountLockoutThreshold>0</AccountLockoutThreshold>
        <AccountLockoutDuration>1</AccountLockoutDuration>
        <User Action="Change" UserID="2">
          <Configuration>
            <UserName><![CDATA[root]]></UserName>
            <Password><![CDATA[]]></Password>
            <RoleId>Administrator</RoleId>
            <Locked>false</Locked>
            <Enabled>Enable</Enabled>
          </Configuration>
        </User>
      </Configuration>
    </Account>
  </NvidiaCfg>
</BmcCfg>
```

Q.1.3.2 DateTime Management

The DateTime sets the BMC clock manually or enables NTP and lists up to six time servers.

- Table Type: OOB
  - Table Name: DateTime
  - XPath: `BmcCfg/NvidiaCfg/DateTime`
  - Sample XML Format:

```
<BmcCfg>
  <NvidiaCfg Action="Change">
    <DateTime Action="Change">
      <Information>
        <DateTime>2025/07/16 09:32</DateTime>
      </Information>
      <Configuration>
        <NTPEnable>Disable</NTPEnable>
        <DateTime>2025/07/16 09:32</DateTime>
        <NTPServer0></NTPServer0>
```

```
          <NTPServer1></NTPServer1>
          <NTPServer2></NTPServer2>
          <NTPServer3></NTPServer3>
          <NTPServer4></NTPServer4>
          <NTPServer5></NTPServer5>
        </Configuration>
      </DateTime>
    </NvidiaCfg>
</BmcCfg>
```

Q.1.3.3 LDAP Management

The LDAP / Active Directory enables external directory authentication and maps remote groups to BMC roles.

- Table Type: OOB
  - Table Name: LDAP
  - XPath: `BmcCfg/NvidiaCfg/LDAP`
  - Sample XML Format:

```
<BmcCfg>
  <NvidiaCfg Action="Change">
    <LDAP Action="Change">
      <Information>
        <CACertificateValidUntil>2026-01-10</CACertificateValidUntil>
        <LDAPCertificateValidUntil>2026-01-10</LDAPCertificateValidUntil>
      </Information>
      <Configuration>
        <ServiceEnabled>Disable</ServiceEnabled>
        <ServiceType>ActiveDirectory</ServiceType>
        <OpenLDAP Action="Change">
          <Configuration>
            <ServiceAddresses>ldap://192.168.34.56</ServiceAddresses>
            <Username></Username>
            <Password></Password>
            <BaseDistinguishedNames></BaseDistinguishedNames>
            <UsernameAttribute></UsernameAttribute>
            <GroupsAttribute></GroupsAttribute>
            <RemoteRoleMapping Action="Change" RuleID="0">
              <Configuration>
                <RemoteGroup><![CDATA[]]></RemoteGroup>
                <LocalRole>None</LocalRole>
              </Configuration>
            </RemoteRoleMapping>
          </Configuration>
        </OpenLDAP>
        <ActiveDirectory Action="Change">
          <Configuration>
```

```
            <ServiceAddresses>ldap://192.168.34.56</ServiceAddresses>
            <Username>root</Username>
            <Password></Password>
            <BaseDistinguishedNames></BaseDistinguishedNames>
            <UsernameAttribute></UsernameAttribute>
            <GroupsAttribute></GroupsAttribute>
            <RemoteRoleMapping Action="Change" RuleID="0">
              <Configuration>
                <RemoteGroup><![CDATA[]]></RemoteGroup>
                <LocalRole>None</LocalRole>
              </Configuration>
            </RemoteRoleMapping>
          </Configuration>
        </ActiveDirectory>
      </Configuration>
    </LDAP>
  </NvidiaCfg>
</BmcCfg>
```

Q.1.3.4 Policies Management

The Policies toggles services such as the SSH BMC shell and network IPMI, and sets the web session timeout.

- Table Type: OOB
  - Table Name: Policies
  - XPath: `BmcCfg/NvidiaCfg/Policies`
  - Sample XML Format:

```
<BmcCfg>
  <NvidiaCfg Action="Change">
    <Policies Action="Change">
      <Configuration>
        <BMCShell>Enable</BMCShell>
        <NetworkIPMI>Enable</NetworkIPMI>
        <SessionTimeout>2 Hours</SessionTimeout>
      </Configuration>
    </Policies>
  </NvidiaCfg>
</BmcCfg>
```

Q.1.3.5 Power Restore Policy Management

The Power Restore Policy decides whether the host stays off, powers on, or returns to its last state after AC is restored.

- Table Type: OOB
  - Table Name: PowerRestorePolicy
  - XPath: `BmcCfg/NvidiaCfg/PowerRestorePolicy`
  - Sample XML Format:

```
<BmcCfg>
  <NvidiaCfg Action="Change">
    <PowerRestorePolicy Action="Change">
      <Configuration>
        <Policy>LastState</Policy>
      </Configuration>
    </PowerRestorePolicy>
  </NvidiaCfg>
</BmcCfg>
```

Appendix R. AD/LDAP Account Login on BMC

You can use Active Directory (AD) and LDAP directory services with BMC for authentication. You can configure it through the BMC web interface or SAA commands. This allows you to log in directly to BMC using SAA and your directory service credentials.

R.1 Configuring AD/LDAP Account Login Settings

Before using AD/LDAP function, you need to configure BMC user settings. Choose one of these methods:

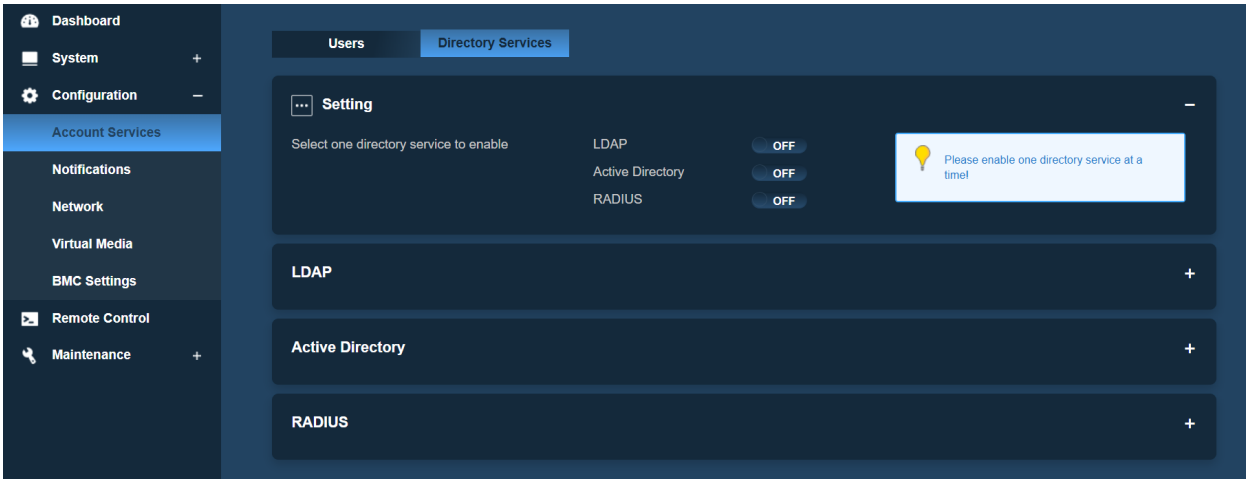
- BMC web interface
- SAA commands

Instructions for both of these methods are provided in the following chapters.

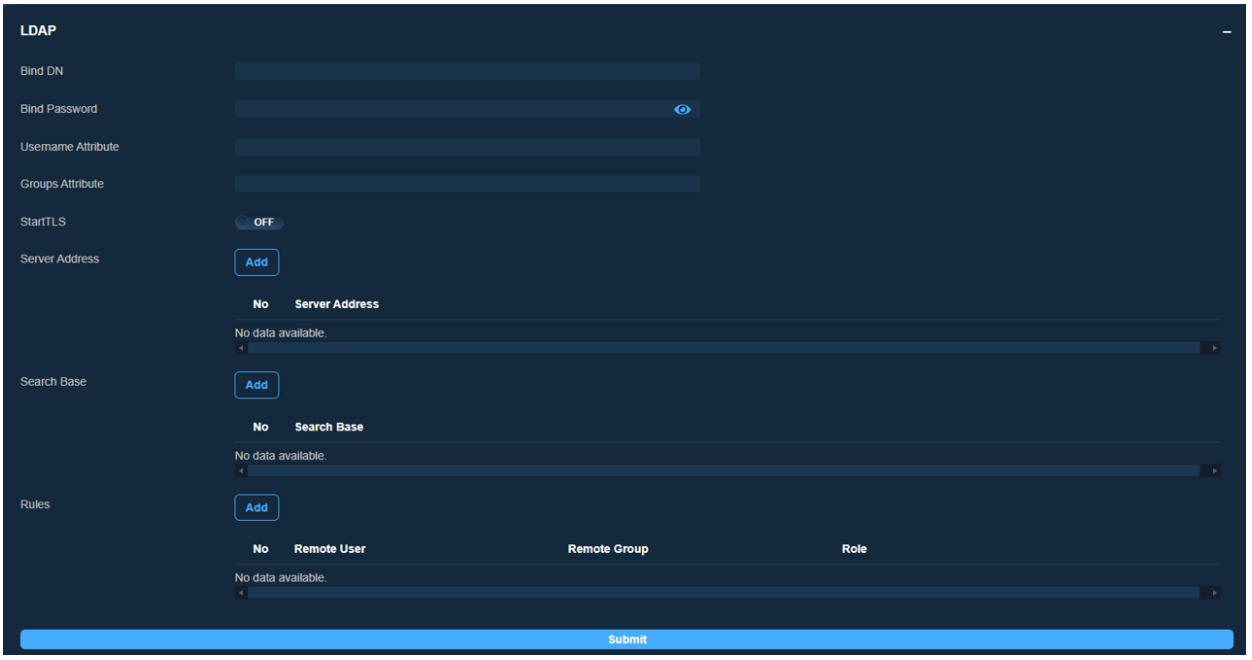
R.1.1 Configuring AD/LDAP Account Login Settings through BMC Web Interface

Follow the steps below to configure the AD/LDAP account login settings through BMC web interface:

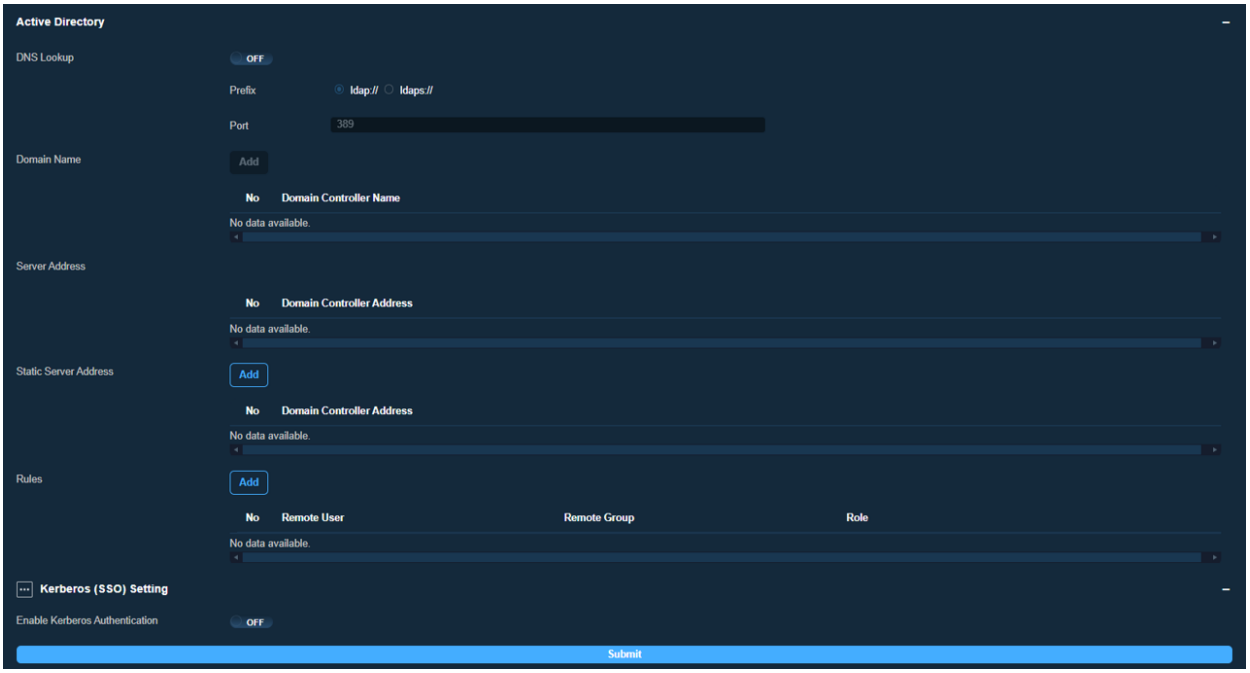
1. Log in to the BMC web interface using administrator privileges.
2. Select Configuration → Account Service → Directory Services.
3. Toggle the Active Directory or LDAP option to `On`.



3a. Enter the **LDAP** account login settings in the BMC web interface.



3b. Enter the **Active Directory** account login settings in the BMC web interface.



R.1.2 Configuring AD/LDAP Account Login Settings through SAA Commands

Follow the steps below to configure the AD/LDAP account login settings through SAA commands:

1. Use the GetBmcCfg command to get the BMC configuration file from BMC.

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

```
File "bmccfg.xml" is created
```

2a. Enter the LDAP account login settings in bmccfg.xml file.
To successfully connect to your LDAP server, you must complete the following fields.

- LDAPEnable: Enables or disables LDAP functionality.
- BindDN: The Distinguished Name for the bind user.
- UsernameAttribute: The attribute used to identify users in the directory.
- SearchBase: The base DN for user searches.
- ServiceAddr: The address of the LDAP service.

- RulePrivilege: Defines the privilege rules for LDAP users.

Note that the LDAP functionality must also be enabled by setting the LDAPEnable field to Enable, otherwise the BMC cannot use the LDAP settings.

```
<LDAP Action="Overwrite">
  <Information>
    <MaximumAvailableADGroup>5</MaximumAvailableADGroup>
    <TotalConfiguredADGroup>1</TotalConfiguredADGroup>
  </Information>
  <Configuration>
    <LDAPEnable>Enable</LDAPEnable>
    <BindDN>cn=abc, dc=def, dc=ghi</BindDN>
    <BindPassword></BindPassword>
    <UsernameAttribute>cn</UsernameAttribute>
    <GroupsAttribute></GroupsAttribute>
    <SearchBase1>dc=def, dc=ghi</SearchBase1>
    <ServiceAddr1>ldap://192.168.34.56:389</ServiceAddr1>
    <ServiceAddr2></ServiceAddr2>
    <ServiceAddr3></ServiceAddr3>
    <LDAPRule Action="Change" RuleID="1">
      <Configuration>
        <RemoteUser><![CDATA[Administrator]]></RemoteUser>
        <RemoteGroup><![CDATA[]]></RemoteGroup>
        <RulePrivilege>Administrator</RulePrivilege>
      </Configuration>
    </LDAPRule>
  </Configuration>
</LDAP>
```

2b. Enter the AD account login settings in bmccfg.xml file.
To successfully connect to your Active Directory server, you must complete the following fields.

- ADEnable: Enables or disables Active Directory functionality.
- UserDomainName: The domain name for AD users.
- RulePrivilege: Defines the privilege rules for AD users.
- DNSLookupEnable or ServiceAddr1: Select one of these to specify the AD server address.
    - DNSLookupEnable and ServiceAddr1 are mutually exclusive fields. You must set one of them, but not both.

- If `DNSLookupEnable` is set to `Enable`, the system will automatically select an AD server via the DNS server. In this case, you do not need to enter a value for ServiceAddr1.
- If `DNSLookupEnable` is set to `Disable`, you must specify the AD server's IP address in the ServiceAddr1 field.

Note that you must enable AD functionality. To do that, set the ADEnable field to "Enable."

```
    <AD Action="Overwrite">
      <Information>
        <MaximumAvailableADGroup>5</MaximumAvailableADGroup>
        <TotalConfiguredADGroup>1</TotalConfiguredADGroup>
        <DynamicServerAddress1></DynamicServerAddress1>
        <DynamicServerAddress2></DynamicServerAddress2>
        <DynamicServerAddress3></DynamicServerAddress3>
        <DynamicServerAddress4></DynamicServerAddress4>
        <DynamicServerAddress5></DynamicServerAddress5>
      </Information>
      <Configuration>
        <ADEnable>Enable</ADEnable>
        <DNSLookupEnable>Enable</DNSLookupEnable>
        <Prefix>ldap</Prefix>
        <Port>389</Port>
        <UserDomainName1>ad.bcd.com</UserDomainName1>
        <UserDomainName2></UserDomainName2>
        <UserDomainName3></UserDomainName3>
        <UserDomainName4></UserDomainName4>
        <UserDomainName5></UserDomainName5>
        <ServiceAddr1></ServiceAddr1>
        <!--Example: ldap://192.168.34.56:389 or ldaps://XXXXXX.com:636-->
        <ServiceAddr2></ServiceAddr2>
        <ServiceAddr3></ServiceAddr3>
        <ADRule Action="Change" RuleID="1">
          <Configuration>
            <RemoteUser><![CDATA[ad_spring]]></RemoteUser>
            <RemoteGroup><![CDATA[cn=season, cn=Users, dc=bcd, dc=com]]>
</RemoteGroup>
            <RulePrivilege>Administrator</RulePrivilege>
          </Configuration>
        </ADRule>
      </Configuration>
    </AD>
```

3. Use the ChangeBmcCfg command to update the BMC configuration file to BMC.

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

```
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
```

R.2 Using AD/LDAP Account Login

After configuring the user settings, you can use SAA commands with AD/LDAP account credentials to log in to BMC directly.
For SAA commands that do **NOT** use **pure** Redfish, you can either use the `--redfish` option or set `redfish_only` to `on` in the `.saarc` file.
For SAA commands that use **pure** Redfish, you can execute commands without above additional settings.

The following table lists the SAA_1.3.0 commands that currently support AD/LDAP account login via pure Redfish. Commands or options that do not support pure Redfish will not allow you to log in. Instead, an error message indicating insufficient privileges appears.

Command Group	SAA Command
Health Management	CheckSensorData
System Management	GetFruInfo
	GetFirmwareInventoryInfo
	UpdateFirmware
	GetSystemInfo
BIOS Management	GetBiosInfo

	UpdateBios
	LoadDefaultBiosCfg
	GetFixedBootCfg
BMC Management	GetBmcInfo
	UpdateBmc
	LoadDefaultBmcCfg
System Event Log	GetEventLog
Storage Management	GetNvmeInfo
Power Management	GetPowerStatus
VM Management	MountIsoImage
	UnmountIsoImage
Security Management	BiosRotManage
	BmcRotManage
	CmmRotManage

The usage supported by each SAA command may vary. Refer to the corresponding section of each command for details.

The following example uses the Pure Redfish command RmcpManage.

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u LDAP_USERNAME -p LDAP_PASSWORD -c
RmcpManage --action 1
```

The console output contains the following information.

```
Managed system.............192.168.34.56
    RMCP Status............Enable
```

```
    RMCP Port.................623
```

Non-pure redfish command — using GetBmcInfo **with --redfish** as an example:

```
[SAA_HOME]# ./saa -i 192.168.34.56 -u LDAP_USERNAME -p LDAP_PASSWORD -c
GetBmcInfo --redfish
```

The console output contains the following information.

```
Managed system...........192.168.34.56
    BMC UFFN.............BMC_X13AST2600-ROT20-D301MS_20250215_01.04.01_STDsp.bin
    BMC type.............X13_RoT2.0_ATEN_AST2600_2_1
    BMC version..........01.04.01
    BMC build date.......2025/02/15
```

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 (General Information)
	support@supermicro.com (Technical Support)
Website:	*www.supermicro.com*

Europe

Address:	Super Micro Computer B.V.
	Het Sterrenbeeld 28, 5215 ML
	's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information)
	support@supermicro.nl (Technical Support)
	rma@supermicro.nl (Customer Support)
Website:	*www.supermicro.nl*

Asia-Pacific

Address:	Super Micro Computer, Inc.
	3F, No. 150, Jian 1st Rd.
	Zhonghe Dist., New Taipei City 235
	Taiwan (R.O.C.)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	*support@supermicro.com.tw*

Website: *www.supermicro.tw*