



SUPERMICRO SERVER MANAGEMENT: BMC FIRMWARE SECURITY

TABLE OF CONTENTS

- Executive Summary 1
- Configure BMC Network Settings with Security 1
- Secure Redfish APIs 6
- BIOS-BMC secure features 6
- Hardware Security 7
- Principles of Secure Software Development Life cycle 7
- Signed firmware and Right Tools from Supermicro 8
- Conclusion 8

SUPERMICRO

Supermicro is a global leader in high performance, high efficiency server technology and innovation that develops and provides end-to-end green computing solutions to the datacenter, cloud computing, enterprise IT, big data, HPC, and embedded markets. Our Building Block Solutions® approach allows us to build and provide a broad range of SKUs that are optimized to individual customer needs and workloads.

Executive Summary

Supermicro server architecture is built on advanced technologies that provide high performance/watt, flexible IO, and management features that allow Enterprises/datacenters/OEMs to achieve the best ROI for their business. One of these technologies is the onboard baseboard management controller (BMC), which provides an efficient interface that enables IT administrators to manage the server's health through temperature/voltage readings and everyday server maintenance tasks like BIOS upgrades and debug OS remotely through KVM consoles.

Configure BMC Network Settings with Security on Supermicro Servers

While this feature increases convenience and productivity, server administrators need to understand that BMCs are embedded controllers with an operating system and network stack that could be vulnerable to attacks if not configured correctly. This feature guide provides several practical use cases for the user to figure out how proper BMC configurations can mitigate vulnerability attacks.



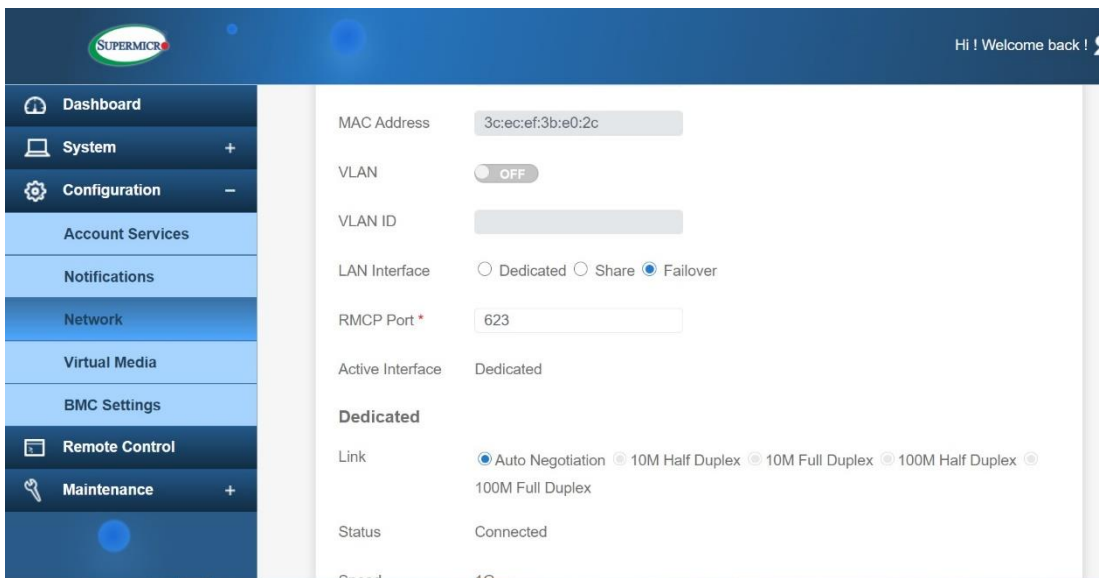
IP Address Assignment

DHCP is the default protocol for receiving IP addresses. However, administrators are encouraged to set static IP addresses or restrict the assignment of DHCP addresses to a secure set of IP addresses or subnet.

LAN Access

The BMC can be accessed through either a dedicated Ethernet LAN interface (if available) or through a shared LAN (System LAN) Interface. The default setting is 'failover,' which means the BMC will first check for the presence of an active, dedicated LAN interface, other it will respond on through a shared LAN interface. The failover setting helps IT administrators receive default connectivity to the BMC, irrespective of their network topology and provision systems remotely. It is recommended that administrators configure BMCs LAN access through a dedicated LAN interface instead of a System LAN. The BMC is not exposed to the internet or unauthorized user access outside of a firewall.

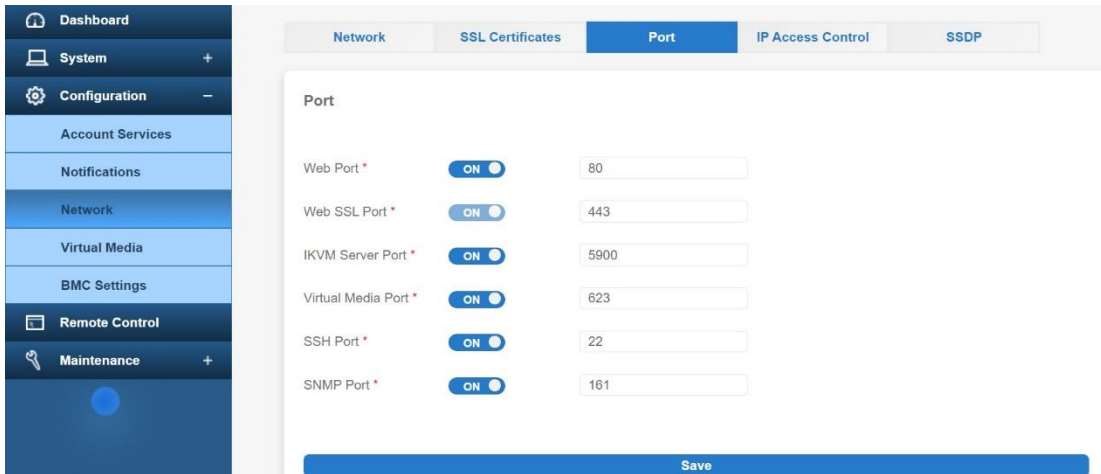
While the IPMI standard protocol defines UDP port 623 for RMCP communications, there are additional remote services that BMCs provide to efficiently provision and debug servers. Some of these services include VNC for debugging an OS, access to http/https ports for BMC settings and reading server health, and Virtual media for remotely accessing files and images.



Note: Unhooking an Ethernet cable from a dedicated LAN interface does not stop accessing BMCs from a shared LAN interface.

Service Ports

All these services run on TCP/UDP ports (please see the security feature guide for the latest information), and it is important to restrict these ports to secure the server management network. Alternatively, the administrator can reconfigure the port numbers or disable unused services to avoid unnecessary security exposure on BMCs. For example, http can be configured to listen on port 76680 such that attackers cannot find the servers through common port scanning tools.

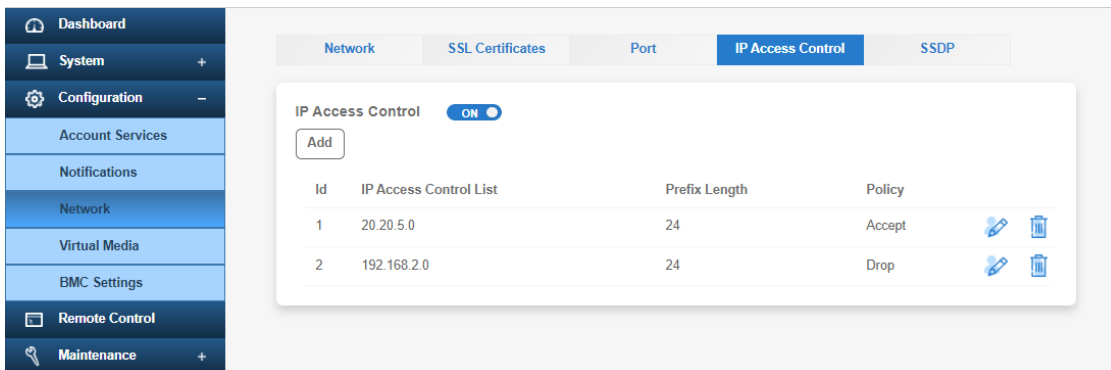


RAKP

IPMI standard dictates using the RAKP protocol to authenticate RMCP sessions between IPMI clients and BMC servers. The current RAKP hash is typically weak, meaning that one can use brute methods to retrieve passwords. The Supermicro BMC provides a stronger hash option for RAKP authentication. Since this is an OEM implementation and may not be suitable in every environment, administrators still recommend blocking UDP port 623 on unsecured networks.

IP Access Controls

BMC access should be restricted to include only known machine IP Addresses. This eliminates unwarranted access to corporate servers from inside the network accidentally or deliberately.



VLAN Configurations

Configure traffic from BMCs to IPMI clients on a unique VLAN so that management traffic can be segregated from the rest of the server data.

Configuring the BMC Network

Though BMCs provide security features to defend against unwarranted attacks, it is strongly recommended that administrators follow the best practice of configuring BMCs on the networks where they are locally accessible and restrict traffic on sensitive ports between networks. Traffic on default ports for BMCs such as TCP/5900 and UDP/ 623 should be restricted to secure and known networks using firewall rules in routers.

BMC management account security

Supermicro BMC provides the following two secure functions to enhance BMC user accounts security and protect from excessive failed login attempts:

1. Authentication failure lockout controls

When user authentication fails, the Supermicro BMC solution can notify the user about the logging fault threshold and deny the user further login authentication, even with the correct password. In addition, the frequency of event logs, the number of failed attempts, and the time for the lockout to expire can be adjusted via the BMC web user interface.

2. Password complexity and value rules

Supermicro BMC solution secures each user account with password complexity, preventing hackers from easily or systematically cracking the user account password. As a result, either IT administrators or ordinary users can enjoy a secured remote management environment provided by the Supermicro BMC solution.

Password Security

Supermicro BMC solution equips every Supermicro product with a preprogrammed BMC management password, which is unique. It requires a user to generate a new means of authentication before access is granted to the device for the first time. This security mechanism can secure customers to have a more secure management environment afterward. More importantly, it can comply with SB-327 law (California Law). Otherwise, Special characters like #,\$ are not allowed into the password field, as these characters can enable shell injection from intruders. Instead, use strong passwords that are at least eight characters long and include a mix of numbers, capital, and lower case letters.

System Lockdown

Supermicro BMC solution can support the System Lockdown feature, and it offers IT administrators a secure way to prevent unintentional system configuration changes. All system configuration changes, including firmware updates, are restricted when system lockdown is enabled. As a result, the ordinary user only receives notifications when the IT administrator makes a system configuration change. System lockdown can be configured by following Supermicro interfaces:

- Web GUI
- IPMI command
- Redfish
- BIOS GUI
- SUM (Supermicro Update Manager)

HTTPS for Web access

Supermicro BMC web server provides HTTPs connection by default to provide both IT administrators and ordinary users a more secure method to access runtime remote management data via the Supermicro BMC solution. HTTPS uses the SSL/TLS protocol to encrypt communications to avoid attackers stealing data. In addition, the Supermicro BMC solution contains SSL/TLS design, preventing impersonations and stopping multiple kinds of cyber attacks.

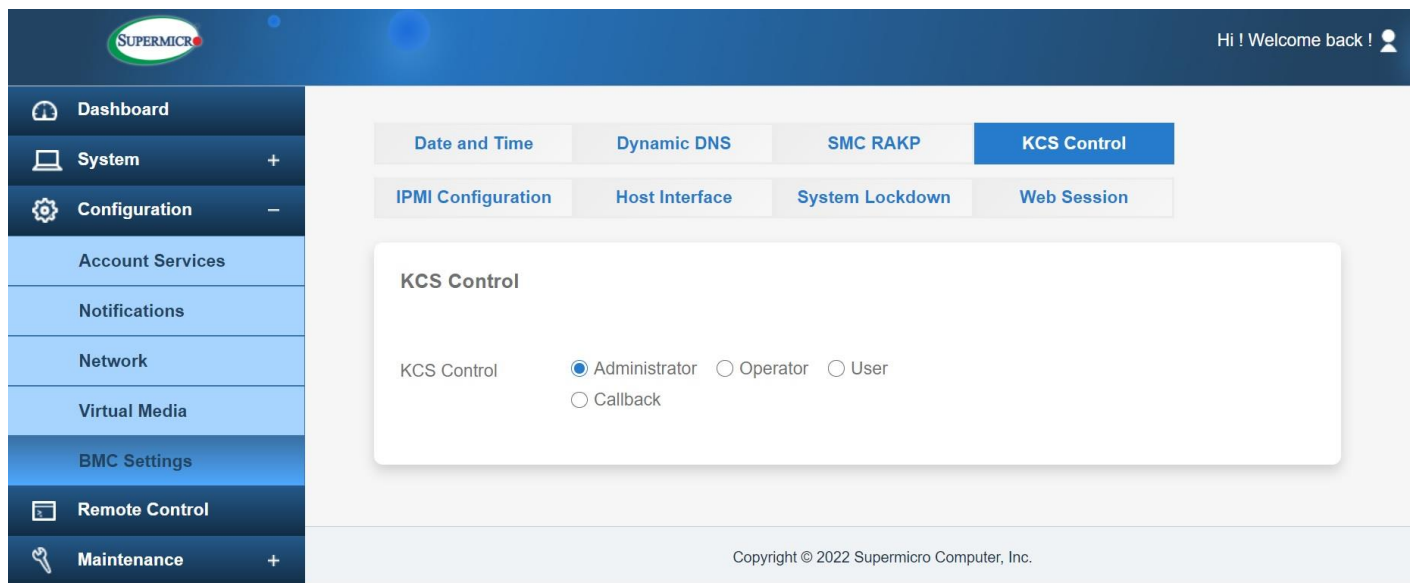
SNMPv3

Supermicro BMC solution also provides a more secure Simple Network Management Protocol Ver. 3(SNMPv3). The biggest security concern in SNMPv1 and SNMPv2 is that community strings are sent as clear-text strings and not encrypted, which means data transmission over SNMPv1 and SNMPv2 is not secure. This security concern has been fixed by SNMPv3 and ensures community strings are always encrypted. IT Administrators can use SNMPv3 on the Supermicro BMC solution directly to make your data center's network environment secure.

KCS Privilege Control

Supermicro BMC solution also enhances the security of legacy IPMI in-band interface – KCS (Keyboard Controller Style). IPMI spec defines the privilege for IPMI Messaging Interface, but it is not applied to the KCS interface since it is a session-less interface. That causes the security issue. To secure the KCS interface, the Supermicro BMC solution offers enhanced features to secure your system inside.

IT Administrators can configure KCS privileges by BMC Web and redfish API.



The screenshot displays the Supermicro BMC web interface. The top navigation bar includes the Supermicro logo and a user greeting "Hi ! Welcome back !". A left sidebar contains menu items: Dashboard, System, Configuration, Account Services, Notifications, Network, Virtual Media, BMC Settings, Remote Control, and Maintenance. The main content area features a top navigation bar with tabs: Date and Time, Dynamic DNS, SMC RAKP, and KCS Control (selected). Below this is a sub-navigation bar with tabs: IPMI Configuration, Host Interface, System Lockdown, and Web Session. The central panel, titled "KCS Control", shows a "KCS Control" label followed by radio button options: Administrator (selected), Operator, User, and Callback. The footer of the interface reads "Copyright © 2022 Supermicro Computer, Inc."

Disallow In-band firmware updates over the KCS interface

This restriction is implemented in the latest Supermicro X12 platforms or later. Disable in-band firmware updates over the KCS interface and only support in-band firmware updates through LAN/USB interface, which is much faster and more secure.

- Detailed conventions:
 - Only Supermicro Update Manager (SUM) can update BIOS and BMC firmware through the BMC in-band interface
 - 3rd party tools (which are NOT validated by Supermicro) will not be allowed to work from Supermicro X12 platforms

Secure Redfish APIs

Supermicro BMC solution also can support DMTF Redfish®. A standard API delivers simple and secure management for converged, hybrid IT and the Software Defined Data Center (SDDC). This modern interface builds on widely-used tools to accelerate development. Today's customers demand a well-defined API that uses the protocols, structures, and security models common in Internet and web services environments.

Secure In-band authentication through the Host interface

Furthermore, the Supermicro BMC solution can support Redfish Host Interface Specification (DSP0270), providing BMC a secure communication channel to the host OS or UEFI.

Main security features include:

- Support authentication, confidentiality, and integrity:
 - Support environments where users do not want to rely on Host/OS access control mechanisms solely
 - Provide a mechanism to optionally (if configured) pass credentials to an OS Kernel for sensor monitoring (with configurable privilege)
- Support security requirements with authentication and confidentiality

BIOS-BMC secure features

Supermicro BMC solution can configure BIOS secure features, Secure Boot, and Secure Drive Erase via Redfish's secure interface. As a result, IT administrators can take advantage of these two security features while provisioning or maintaining a system.

- Secure Boot

Secure boot is part of the UEFI firmware standard (since 2.3.1c). A machine refuses to load any UEFI driver or app with secure boot enabled unless the operating system bootloader is cryptographically signed.

- Secure Drive Erase

IT administrators can apply an action to erase the disk connected with the Broadcom MegaRAID controller, and it allows IT administrators to render data on attached drives instantly and securely.

Due to its secure data removal and cleansing, secure drive erase can comply with the most stringent privacy laws and meet the most rigorous security requirements in the world as those set up by the State of California and the European Union.

Hardware Security

As security protections advance, attacks become increasingly sophisticated, including targeting the low-level platform firmware, such as BIOS and BMC. Supermicro follows industry guidelines – NIST 800-193, Platform Firmware Resiliency Guidelines, introduced by the National Institute of Standards and Technology (NIST) to design Firmware Resilient Platform. A resilient firmware system begins with a platform Root-of-Trust(RoT). Supermicro RoT is a hardware-based solution that protects the various low-level platform firmware components from remote attacks. The protected duration includes each system AC on, firmware update, and runtime. The key firmware components on the system, including BIOS, BMC, and CPLD, are all under RoT protection.

Secure Firmware Updates and Restoration through RoT

Supermicro RoT solution verifies the integrity of platform firmware images before the firmware is updated. And most important, it can even restore corrupted firmware automatically from a protected known-good recovery image. It provides IT Administrators additional options to protect low-level platform firmware with the Supermicro RoT solution.

Runtime Protections through Trust Zone (TEE OS)

Supermicro solution utilizes the Trust-Zone capability in BMC ARM processor to check the integrity of BMC applications and processes during runtime. Trust-Zone (TEE OS) provides an isolated processing environment in which Trusted Applications can be securely executed irrespective of the rest of the environment in BMC.

Principles of Secure Software Development Life cycle to harden the firmware security

Supermicro solution is committed to taking our Software Development Life Cycle (SDLC) to the next level: the Secure Software Development Life Cycle (SSDLC). Considering the possible risk from a broad network connection scenario, we have enhanced our products and solutions during product development lifecycle management to provide appropriate features or configurations to IT Administrators for managing data centers with secured deployment. Supermicro has adopted the following security practices in our development lifecycle framework:

- **Inter-section Participants:** different roles and duties regarding security development management were assigned to the Developer, Software Security team, and Software Product Manager.
- **Security Requirement and Risk Assessment:** The requirements from relevant stakeholders and the risk from possible applications must be evaluated while the product lifecycle is initiated.
- **Security design and development analysis:**
 - The open-source package for software was analyzed during the product development phase.
 - Threat modeling methodology was adopted for impact analysis.
 - An automatic tool such as a source code scanner, code repository, and issue tracking was applied for secure coding.
- **Independent Security testing and validation:**
 - Supermicro's Software Security team has employed security testing with both static and dynamic analysis criteria to discover known and unknown vulnerabilities. In addition, Supermicro has employed different testing tools regarding Vulnerability Scan, Penetration testing, and Fuzz testing.
 - When security issues with high priority are found, it is necessary to bring out the mitigations and then verify by the Software Security team before product release. Issues with medium or low priority will be scheduled to fix according to the Supermicro development roadmap.

- **Security Deployment and Maintenance:**

- IT administrators for secured deployment should follow written network settings and system configurations. In addition, Supermicro has initialized a plan of firmware updates for our customers to respond to possible vulnerabilities. Supermicro highly recommends that IT administrators follow a plan of a periodic firmware update to avoid security issues.
- Supermicro has initialized a public security center, where customers can report a security issue in time and update the status of responses regarding security issues.

Moreover, Supermicro will keep monitoring the latest cybersecurity framework, such as Secure Software Development Framework (SSDF) and Cybersecurity Maturity Model Certification (CMMC), to fulfill different aspects of security requirements regarding SSDLC.

Signed firmware and Right Tools from Supermicro

Cryptographically signed firmware

Supermicro BMC, BIOS, motherboard CPLD, and Chassis Management Module's latest solutions use the CNSA algorithms to realize cryptographically signed firmware. Commercial National Security Algorithm (CNSA) Suite is published by the United States Government, which defines cryptographic algorithm policy for national security applications.

Plan for periodic firmware updates

Supermicro releases periodic firmware updates that add new security features and provide fixes for issues on an ongoing basis. In addition, Supermicro fixes high priority issues on its developed technologies and for many underlying components included in its products, such as OpenSSL.

Hence, it is a collective responsibility of vendors and users of products to work together and ensure that the servers are updated and secured in deployments.

Please go to the Supermicro Security Center for the latest CVEs and information at https://www.supermicro.com/en/support/security_center

Using the Right Tools

Supermicro provides several options to upgrade and provision BMC firmware depending on the server deployment size, environment (e.g., datacenter vs. an appliance in-network), operator's choice of CLI or WebUI interfaces, etc.

Some common tools available on the website are Supermicro Server Manager (SSM), Supermicro Update Manager (SUM), SMCIPMITOOL, IPMICFG, and IPMIView, which can all be downloaded from <https://www.supermicro.com/sms>

Conclusion

Supermicro design continuously offers convenient, secure, and diversified remote management interfaces and methods designed in our Baseboard Management Controllers (BMC) solution. It provides IT administrators modern and efficient system manageability, including:

- Web GUI
- IPMI command
- Redfish
- Supermicro System Management Software (SSM, SUM ...etc.)

Because of the BMC's powerful capabilities, it is recommended that server administrators take advantage of the security features that BMCs offer while restricting network access to the BMC on a protected subnet behind a firewall. BMC Security is an evolving topic. Supermicro has been actively working with the IT security community and customers to provide timely firmware updates that continuously improve the security of Supermicro products. Supermicro recommends planning for regular firmware upgrades and employing the right set of tools to make upgrades and configurations easy.