Intel® Server Systems Baseboard Management Controller (BMC) and BIOS Security

Intel Best Practices White Paper

Revision 1.2

January 2021

Intel® Server Boards and Systems

<Blank Page>

Revision History

Date	Revision Number	Modifications
August, 2016	1.0	Initial release
October, 2019	1.1	Adding information about protecting KCS interface
January, 2021	1.2	New password complexity rules Minor updates throughout for clarity

Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Table of Contents

This page intentionally left blank

1. Overview

On Intel® Server Boards and Systems, the Baseboard Management Controller (BMC) and Basic Input/Output System (BIOS) have several features that allow for additional security in the data center. This paper focuses on the best actions for enabling security on an Intel® Server Board and System.

This paper covers the following systems.

- Purley
    - Intel® Server Board S2600WF Family
    - Intel® Server Board S2600BP Family
    - Intel® Server Board S2600ST Family
    - Intel® Server Board S2600WK Family
- Grantley
    - Intel® Server Board S2600WT Family
    - Intel® Server Board S2600KP Family
    - Intel® Server Board S2600TP Family
    - Intel® Server Board S2600CW Family
- Romley
    - Intel® Server Board S2600GZ Family
    - Intel® Server Board S2600JF Family
    - Intel® Server Board S2600CP Family
    - Intel® Server Board S2600IP Family
    - Intel® Server Board S2600WP Family
- Single Socket
    - Intel® Server Board S1200RP Family
    - Intel® Server Board S1200SP Family

2. Firmware Updates

2.1 Signed BMC

The BMC images for Intel® Server Systems are digitally signed by Intel confirming origination. The BMC is designed to prevent any update of an image that has an invalid signature and on every boot this signature is verified again to help ensure nothing was modified during run time.

2.2 Firmware update best actions

Intel recommends that users flash the latest BMC and BIOS images on the system. Even if the release notes do not explicitly state a security update there may be updates or new features that make the system more secure.

The BIOS and BMC from Intel® Server Systems have a security version in them. Users can downgrade BIOS and BMC versions but will not be allowed to downgrade to a BIOS or BMC that has a lower severity version in it.

After the update is performed, it is recommended that users immediately reboot the system. While the BMC will be updated immediately, the BIOS is staged waiting for the next reboot.

Users can download update packages known as SUP's from the following URL.

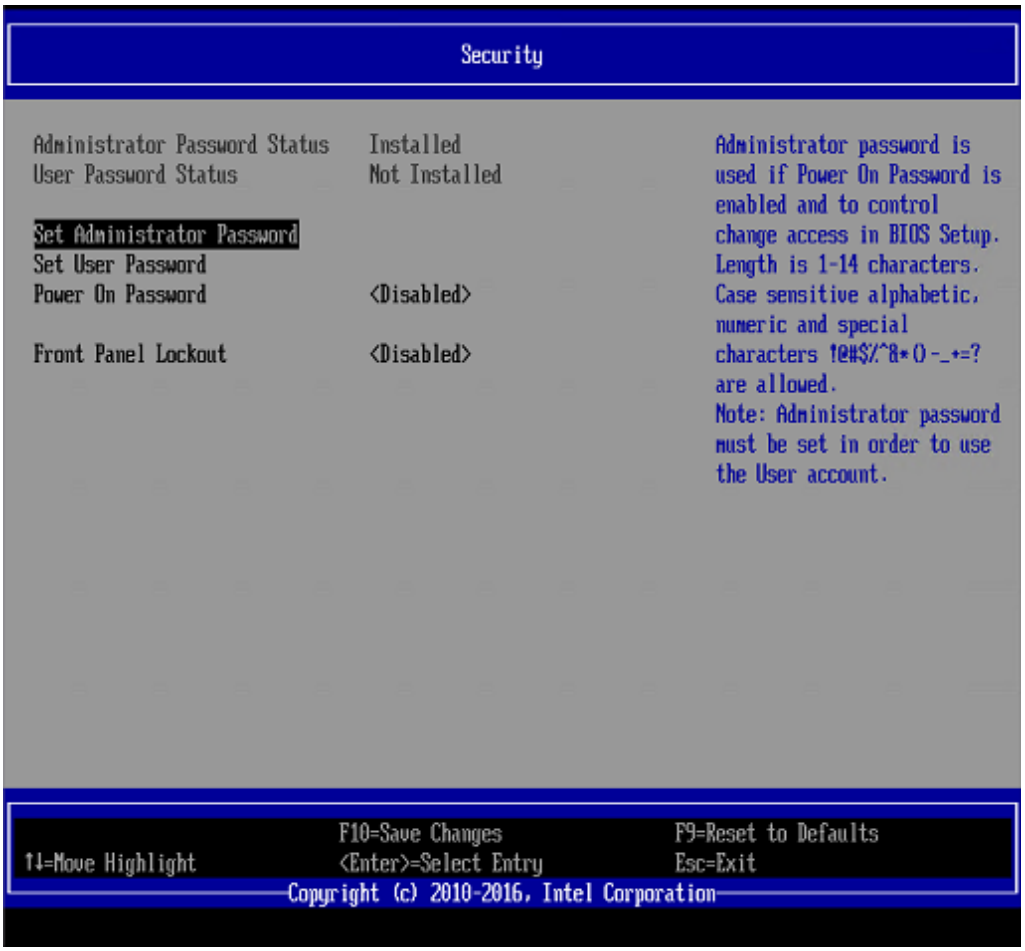
https://downloadcenter.intel.com/product/1201/Server-Products

3. BIOS Features and Settings

3.1 Administrator Password

Users can set an administrator password in BIOS Setup that is designed to prevent users from modifying BIOS settings if they do not know the password. It is recommended that users set this password.

The password will be requested from the user before entering BIOS setup.



3.2 UEFI Secure Boot

UEFI Secure Boot defines how a platform's firmware can authenticate a digitally signed UEFI image, such as an operating system loader or a UEFI driver stored in an option ROM, thus providing the capability to help ensure that those UEFI images are only loaded in an owner authorized fashion and providing a common means to help ensure platforms security and integrity over systems running UEFI-based firmware. Intel® Server Board BIOS is compliant to UEFI specification 2.3.1 Errata C for UEFI secure boot feature. For more details, refer to UEFI specification chapter 27.

For UEFI Secure Boot to work, the boot mode must be set to UEFI in BIOS setup. By default the boot mode is listed as legacy and as a result UEFI Secure Boot is disabled. If user switches boot mode to UEFI, they will see Secure Boot Configuration listed as shown below.

Intel recommends booting with UEFI and enabling UEFI secure boot.

3.3 Intel® Virtualization Technology

Intel® Virtualization Technology consists of three components, which are integrated and interrelated, but, which address different areas of Virtualization.

- Intel® Virtualization Technology ***(VT-x)*** is processor-related and provides capabilities needed to provide a hardware assist to a Virtual Machine Monitor (VMM).
- Intel® Virtualization Technology for Directed I/O (***VT-d)*** is primarily concerned with virtualizing I/O efficiently in a VMM environment.
- Intel® Virtualization Technology for Connectivity (***VT-c)*** is primarily concerned with I/O hardware assist features, complementary to but independent of VT-d.

Intel® VT-x is designed to support multiple software environments sharing same hardware resources. Each software environment may consist of OS and applications. The Intel® Virtualization Technology features can be enabled or disabled in the BIOS setup. The default behavior is disabled. When enabling a power cycle is required. This is a security protection to require physical presence when enabling this functionality.

If not using virtualization, it is recommended to leave this feature disabled.

3.4 Intel® TXT

Intel® Server Systems support Intel® Trusted Execution Technology (Intel® TXT), which is a robust security environment designed to help protect against software-based attacks. Intel® Trusted Execution Technology integrates new security features and capabilities into the processor, chipset, and other platform components. When used in conjunction with Intel® Virtualization Technology and Intel® VT for Directed IO, with an active TPM, Intel® Trusted Execution Technology provides hardware-rooted trust for your virtual applications.

For more information on Intel® TXT, read the whitepaper at
http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html

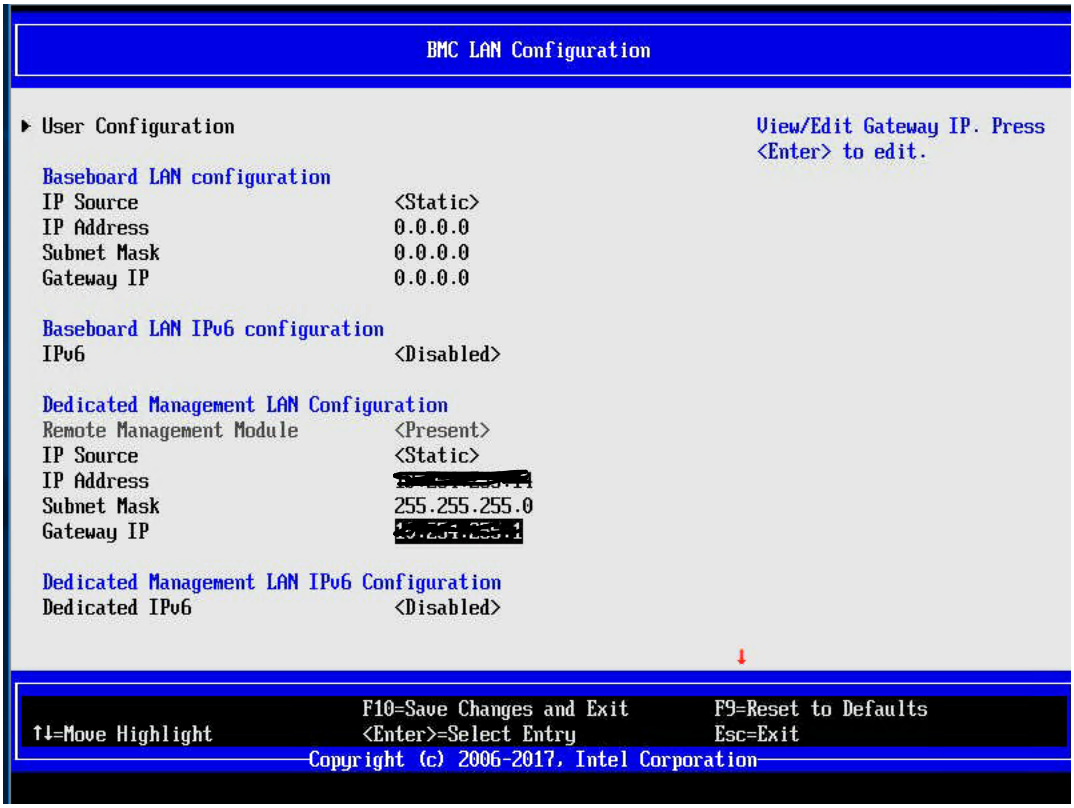
4. BMC Settings and Features

4.1 Networking (w/ Dedicated Management NIC)

It is recommended that the user set up an isolated network for manageability and not expose that network to the internet.

The easiest way to do this is to use a dedicated management NIC. This is considered channel 3 to the BMC, and all IP settings should use channel 3. In BIOS setup, it is listed as the Dedicated Management NIC and can be configured on the screen below.

If an onboard NIC is required, Intel recommends setting up VLAN's to help prevent unauthorized users. VLAN's can be configured in the Integrated BMC Web Console.

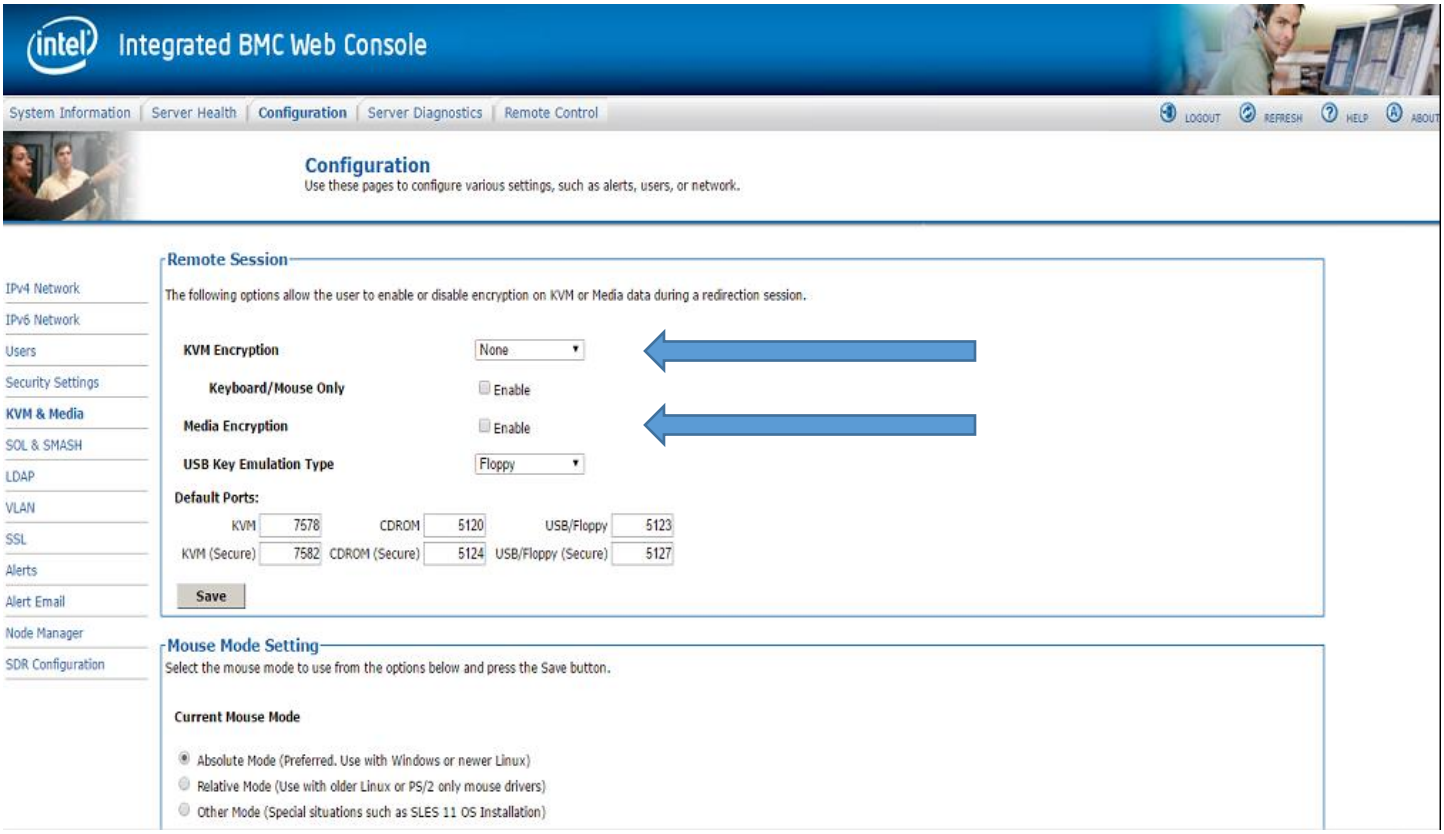


4.2 Encrypt traffic

It is recommended that users enable encryption. With IPMI traffic, users can set up encryption for all IPMI traffic or only serial-over-LAN (SOL).

As SOL can contain entering of user names and passwords, using encryption for at least SOL is highly recommended.

It is also possible to use encryption for KVM and vMedia. Users can do this in the Integrated BMC Web Console shown below.



4.3 Use Cipher Suite 17

It is recommended that users disable all cipher suites other than 17 in the BMC. The easiest way to do this is via ipmitool using the command syntax below.

- Ipmitool –H <ip> -U <username> -P <password> -I lanplus lan set <lan #> cipher_privs XXXXXXXXXXaXXXX

Once done, to continue using ipmitool, users must specify the cipher suite in the arguments.

- Ipmitool –H <ip> -U <username> -P <password> -I lanplus –c 17 chassis status

Note: ipmitool version 1.1.18 or later required to use cipher suite 17

Note: On Intel® Server Systems, the default authentication is callback (limits user to very few calls) if cipher suite 0 is used.

4.4 User configuration

IPMI defines user access by the following levels. If a user needs only limited access, consider giving that user a reduced privilege level.

- Callback
- User

- Operator
- Administrator

Always use strong passwords. IPMI allows up to 20 characters. The following are standard password recommendations to be considered.

- Maximize length. IPMI allows up to 20 characters for passwords.
- Do not use personal information
- Use upper and lower case, numbers and symbols. IPMI allows full ASCII characters
- Do not use words in dictionary
- Avoid simple adjacent keyboard combinations
- Try and change password frequently.

IPMI allows for an anonymous user account with no password. Intel does not recommend using this user account.

4.5 Security Settings in Web Server

The BMC web console has several settings to help improve security of the system. It is recommended that each of these settings be considered.

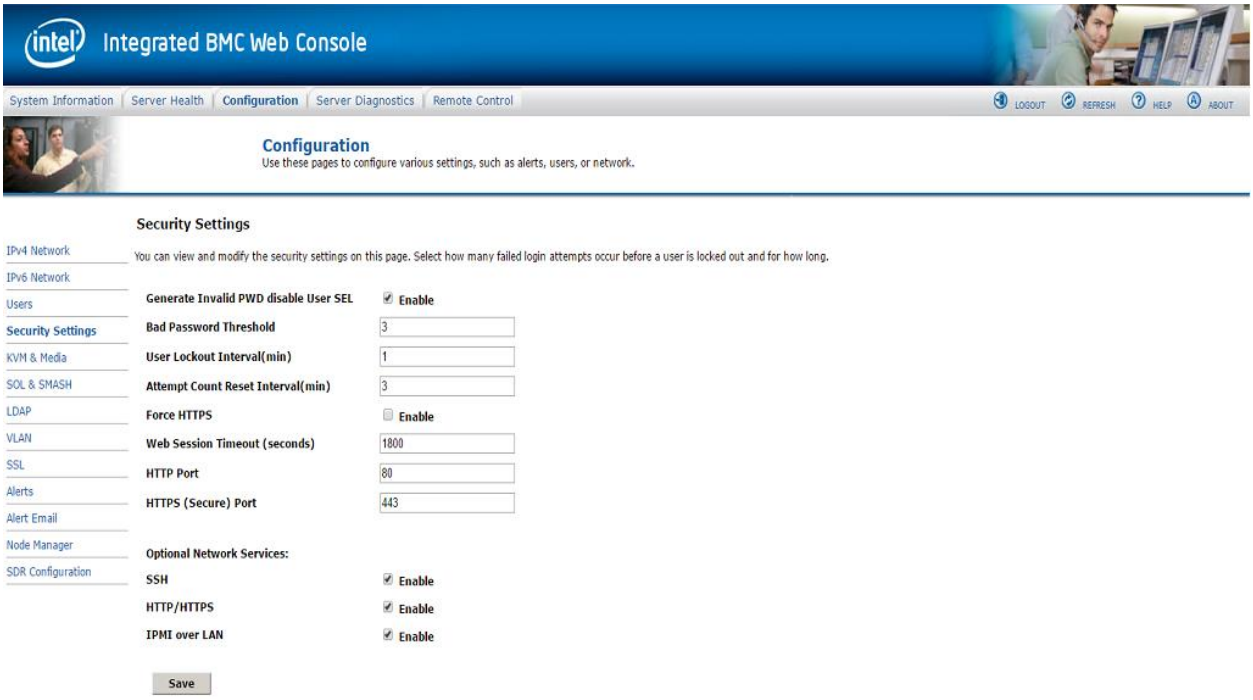
Specifically, it is recommended that customers force HTTPS. Checking Enable in the Force HTTPS box essentially disables HTTP access and only allows the user to use HTTPS.

Note that on Purley and newer systems, only HTTPS is supported.

Users are allowed to change the HTTP port and HTTPS port so that scanners will not detect this as a BMC port.

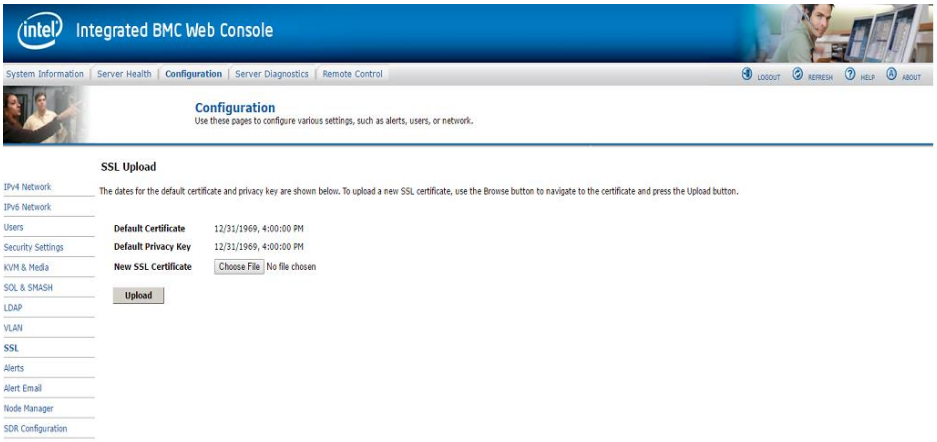
If a user is going to use only one or two of the network features (SSH, HTTP/S, IPMI), it is recommended they disable any features not used.

Note: Disabling "IPMI over LAN" does not impact in-band IPMI traffic.



4.6 Upload a trusted certificate with host certificate verification

It is recommended that users upload their own SSL certificate. A trusted certificate with host certificate verification enabled on the client/browser helps to protect against a host spoofing or man-in-the-middle attack.



4.7 Change KCS Policy Control Mode to “Deny All” after provisioning is complete (Purley BMC 1.99 and later versions only)

After configuring the BMC for out-of-band access, if no further in-band commands will be sent over KCS interface, change the KCS Policy Control Mode to “Deny All”.

The following are the three modes the KCS Policy Control can be set to.

KCS Policy Control Mode – Allow All

This configuration setting is intended for normal IPMI compliant communications between the Host OS and the BMC. This mode should be used when provisioning the BMC configuration for deployment.

KCS Policy Control Mode – Deny All **RECOMMENDED**
This configuration setting disables the IPMI KCS command interfaces between the Host OS and the BMC. This is a non-compliant IPMI configuration that will impact the operation of the Server Management Software running on the Host OS. This only applies to the IPMI commands over the KCS interfaces, and does not apply to the authenticated network interfaces to the BMC.

KCS Policy Control Mode – Restricted
Important Note: As restricted mode will still allow a BMC firmware downgrade, the system can be downgraded to an older version that does not have this mode, thus placing the system in allow all mode.

This configuration setting enables the use of an Access Control List by the BMC Firmware that allows applications executing on the host OS to have access to a limited set of IPMI commands using the KCS interfaces. This is a non-compliant IPMI configuration that may impact the operation of the Server Management Software running on the Host OS. For example, the IPMI commands that are used to provision the BMC configuration settings, or control the state of the Host OS, will be disallowed when the BMC KCS interface is in restricted mode. This only applies to the IPMI commands over the KCS interfaces, and does not apply to the authenticated network interfaces to the BMC.

Note: By default there is no BMC IP, username, and password. Make sure an IP address, username, and password is entered prior to going into one of these modes as all commands will be rejected by both utilities and BIOS setup. BIOS also uses this KCS interface, so if setting to "Deny All", the BIOS will be unable to communicate with the BMC after POST and users will not see events that come from BIOS.

The current mode will be displayed in the embedded web console if the user is in allow all mode.

Note: The Set policy mode is blocked in deny all or restricted mode so current setting must be "allow all" for any of the following commands to work when issued over the KCS interface.

To change the Policy Control Mode to "Deny All", issue the following IPMI command via KCS interface or out-of-band

```
ipmitool raw 0x30 0xB4 0x05
```

or

```
ipmitool –H <ip> -U <user> -P <password> -I lanplus -c 17 raw 0x30
0xB4 0x05
```

To change the Policy Control Mode to “Restricted”, issue the following IPMI command via KCS interface or out-of-band

```
ipmitool raw 0x30 0xB4 0x04
```

or

```
ipmitool –H <ip> -U <user> -P <password> -I lanplus -c 17 raw 0x30
0xB4 0x04
```

To change the Policy Control Mode back to “Allow All”, issue the following IPMI command ***only via authenticated out-of-band*** session.

```
ipmitool –H <ip> -U <user> -P <password> -I lanplus -c 17 raw 0x30
0xB4 0x03
```

4.8 Change Password Complexity Rules to Medium or High (Purley BMC 2.48. ce3e3bd2 and later versions only)

It is recommended that users set BMC complexity rule to Medium or High. This feature, which can only be set by administrator user forces rules on how other create BMC passwords. The following are the settings and rules for each.

Low

* Contains printable characters only

* Password length should be 6 characters or longer

* Meets a minimum of 3 of the following criteria:

    1. Contains upper case

    2. Contains lower case

    3. Contains digit numbers

    4. Contains symbols

* Cannot contain user name (example: if username = Hello, Password=th12(heLLo) is not allowed)

Medium

* Contains printable characters only

* Password length should be 8 characters or longer

* Cannot be the same as the user name or the user name in reverse order.

* Must have at least two new characters when compared with the previous password.

* Meets following 4 criteria:

    1. Contains upper case

    2. Contains lower case

3. Contains digit numbers

4. Contains symbols

High

* Contains printable characters only

* Password length should be 8 characters or longer

* Meets following 4 criteria:

1. Contains upper case

2. Contains lower case

3. Contains digit numbers

4. Contains symbols

* Cannot contain user name (example: if username = Hello, Password=th12(heLLo) is not allowed)

* Cannot contain 3 or more sequential digits in a row (e.g. BMC(123)ste, BMC(654)sfc are not allowed)

* Cannot contain 3 or more sequential alphabet characters in a row (e.g. (AbC) 3478!, 57$(DeF)68k are not allowed))

* Cannot contain 4 or more consecutive characters in a row (e.g. (Fher)145! are not allowed))

* Cannot contain 4 or more consecutive digits in a row (e.g. Fgke(1245)#@, (4390)FGL$ are not allowed)

* Cannot contain 4 or more of the same characters (case insensitive) (e.g. Fkr4fcpF&f (4 'f' or 'F'), Glg5gt2G! (4 'g' or 'G') are not allowed)

4.9 Monitor for Chassis intrusion events

Intel® Server Systems have many sensors that are monitored by the BMC. On most systems, which use a chassis from Intel, one of these sensors is known as the chassis intrusion sensor. Anytime the chassis is opened, this sensor causes a log to be entered in the System Event Log (SEL) of the BMC. Either ensure Management Software is alerting off this event or set up an SNMP or SMTP alert based on this SEL.

Glossary

This appendix contains important terms used in the preceding chapters.

Term	Definition
ACPI	Advanced Configuration and Power Interface
BIOS	Basic Input/Output System
BMC	Baseboard management controller.
IPMI	Intelligent Platform Management Interface
LAN	Local area network
MD2	Message Digest 2 – Hashing Algorithm
MD5	Message Digest 5 – Hashing Algorithm – Higher Security
NIC	Network interface card
SEL	System event log