Securing Intel® Server Systems Baseboard Management Controller and BIOS

<Blank Page>
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>August, 2016</td>
<td>1.0</td>
<td>Initial release</td>
</tr>
<tr>
<td>October, 2019</td>
<td>1.1</td>
<td>Adding information about protecting KCS interface</td>
</tr>
</tbody>
</table>
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.

© Intel Corporation
Table of Contents

1. Overview ................................................................................................................................. 1
2. Firmware Updates .................................................................................................................... 2
   2.1 Signed BMC ....................................................................................................................... 2
   2.2 Firmware update best practices ......................................................................................... 2
3. BIOS Features and Settings ..................................................................................................... 3
   3.1 Administrator Password ................................................................................................. 3
   3.2 UEFI Secure Boot ............................................................................................................. 3
   3.3 Intel® Virtualization Technology ..................................................................................... 4
   3.4 Intel® TXT (w/ Intel® CIT) .............................................................................................. 5
4. BMC Settings and Features ..................................................................................................... 6
   4.1 Networking (w/ Dedicated Management NIC) ................................................................. 6
   4.2 Encrypt traffic .................................................................................................................... 6
   4.3 Use Cipher Suite 17 ........................................................................................................ 7
   4.4 User configuration ............................................................................................................ 8
   4.5 Security Settings in Web Server ..................................................................................... 8
   4.6 Upload a trusted certificate with host certificate verification ......................................... 9
   4.7 Change KCS Policy Control Mode to “Deny All” .......................................................... 10
   4.8 Monitor for Chassis intrusion events .............................................................................. 11
Glossary ........................................................................................................................................ 12

Table of Figures

Figure 1. BIOS security menu ........................................................................................................ 3
Figure 2. Advanced boot options menu ....................................................................................... 4
Figure 3. BMC Lan Configuration menu ..................................................................................... 6
Figure 4. Integrated BMC web console screen ........................................................................... 7
Figure 5. BMC web console security settings ............................................................................ 9
Figure 6. BMC web console SSL upload menu ......................................................................... 9
Figure 7. BMC web console summary screen ............................................................................ 10
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 best practices 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, verifying the signature on each boot to ensure nothing was modified during run time.

2.2 Firmware update best practices

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, Intel recommends to immediately reboot the system. While the BMC is updated immediately, the BIOS is staged waiting for the next reboot.

Users can download update packages known as SUP’s from the following URL:

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. Intel recommends for users to set this password, as the password is requested from the user before entering BIOS setup.

![BIOS security menu](Image)

Figure 1. BIOS security menu

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 method to help ensure platform security and integrity over systems running UEFI-based firmware. The Intel® Server Board BIOS is compliant to UEFI specification 2.3.1 Errata C for the UEFI secure boot feature. For more details, please refer to Chapter 27 in the UEFI specification.

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 the boot mode is switched to UEFI, Secure Boot Configuration is listed as shown below.

**Note:** Intel recommends booting with UEFI and enabling UEFI secure boot.
3.3 Intel® Virtualization Technology (Intel® VT-x)

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. This would generally be a chipset I/O feature but in the Fourth Generation Intel® Core™ Processor Family there is an Integrated I/O unit embedded in the processor, and the IIO is also enabled for VT-d.

- Intel® Virtualization Technology for Connectivity (VT-c) is primarily concerned with I/O hardware assistance 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 an OS and applications. Intel® Virtualization Technology features can be enabled or disabled in the BIOS setup, with the default behavior set to disabled. When enabling, a power cycle is required. This is a security protection to require physical presence when enabling this functionality.

**Note:** If not using virtualization it is recommended to leave this feature disabled.
3.4 Intel® TXT (w/ Intel® CIT)

Intel® Xeon® Processor E5 2600 Product Families 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.

Intel® Cloud Integrity Technology leverages Intel® TXT to provide a root of trust in the datacenter, enabling software-controlled visibility and policy enforcement of hardware-secured asset tags and launch-time measurements of the BIOS, Operating System (OS), and hypervisor. The trust and asset tag attestation information can then be used to provide workload verification, remediation, reporting, and compliance in both public and private cloud environments.

For more information on Intel® TXT, read the whitepaper at:

For more information on Intel® CIT, read the product guide at:
4. **BMC Settings and Features**

4.1 **Networking (w/ Dedicated Management NIC)**

Intel recommends the setup of an isolated network for manageability and to not expose that network to the internet.

To do this, use a dedicated management NIC. On Romley servers, users can purchase the RMM3 module, which allows them to plug in a 3rd dedicated management NIC. On Grantley and Purley based servers, the dedicated management NIC is usually down on the board. In either case, this is considered a 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.

![BMC LAN Configuration](image)

**Figure 3. BMC Lan Configuration menu**

4.2 **Encrypt Traffic**

Intel recommends the enabling of encryption. With IPMI traffic users can set up encryption for all IPMI traffic or only serial-over-LAN (SOL).

**Note:** As SOL can contain entering of user names and passwords, using encryption for SOL is highly recommended.
It is also possible to use encryption for KVM and vMedia. This is accessible in the Integrated BMC Web Console shown below.

![Integrated BMC Web Console](image)

**Figure 4. Integrated BMC web console screen**

### 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 XXXXXXXXXXXXaXXX
```

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

**Note:** `ipmitool` version 1.1.18 or later required to use cipher suite 17
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
- Make use of 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 disables HTTP access and only allows the user to use HTTPS.

**Note:** 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

Intel recommends 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**
  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.

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.

![Figure 7. BMC web console summary screen](image)

**Note:** The set policy mode is blocked in deny all or restricted mode, so the current setting must be set to allow all for any of the following commands to work when issued over the KCS interface.
Securing Intel® Server Systems Baseboard Management Controller and BIOS

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 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. Any time 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACPI</td>
<td>Advanced Configuration and Power Interface</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic input/output system</td>
</tr>
<tr>
<td>BMC</td>
<td>Baseboard management controller.</td>
</tr>
<tr>
<td>IPMI</td>
<td>Intelligent Platform Management Interface</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network</td>
</tr>
<tr>
<td>MD2</td>
<td>Message Digest 2 – Hashing Algorithm</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5 – Hashing Algorithm – Higher Security</td>
</tr>
<tr>
<td>NIC</td>
<td>Network interface card</td>
</tr>
<tr>
<td>SEL</td>
<td>System event log</td>
</tr>
</tbody>
</table>