



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

Good Security Practices White Paper

Revision 1.0

September 2016

Intel® Server Boards and Systems

Revision History

Date	Revision Number	Modifications
September, 2016	1.0	Initial release

Disclaimers

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document may contain information on products, services and/or processes in development. All information provided here is subject to change without notice.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

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

© Intel Corporation

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 higher security in the data center. This paper focuses on good practices for enabling security on an Intel® Server Board and System.

This paper covers the following systems.

- Intel® Server Boards Based on the Intel® Xeon® Processor E5-2600 v3 and v4 Product Family
 - Intel® Server Board S2600WT Family
 - Intel® Server Board S2600KP Family
 - Intel® Server Board S2600TP Family
 - Intel® Server Board S2600CW Family
- Intel® Server Boards Based on the Intel® Xeon® Processor E5-2600 v1 and v2 Product Family
 - 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
- Intel® Server Boards Based on the Intel® Xeon® Processor E3-1200 v3, V4 and v5 Product Family
 - Intel® Server Board S1200RP Family
 - Intel® Server Board S1200SP Family

2. BMC and BIOS good practices

- 2.1 Always flash the latest BMC and BIOS images as they are released from Intel even if the release notes do not explicitly state a security fix.
- 2.2 Use the Administrator Password in BIOS setup.
- 2.3 Use strong passwords for IPMI user accounts and BIOS administrator password.
- 2.4 Enable UEFI Secure boot and TXT when using virtualization.
- 2.5 Intel HW Virtualization technology is off by default. If needed, ensure that your BIOS is trusted and signed, then turn on the VT option in BIOS options on your system. If you are not using Virtualization, then keep this option turned off.
- 2.6 Set up an isolated network for manageability and never expose that network to the internet.
- 2.7 If using onboard NICs for manageability is required, configure VLANs to isolate it from the host network.
- 2.8 Use clients that use or have an option for encryption.
- 2.9 Avoid any client tools that makes use of or have options for Cipher Suite 0.
- 2.10 If possible change the default ports for the web console.
- 2.11 Use the force HTTPS option in the web console.
- 2.12 Disable IPMI in web console if not using it.