

Intel® 8 Series Chipset Family – Intel® Management Engine 9.0 SKU

1.5 MB Firmware Getting Started User Guide

January 2013

Revision 1.0

Intel Confidential



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained at <http://www.intel.com/design/literature.htm>.

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_number for details.

No system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) requires an enabled chipset, BIOS, firmware and software, and a subscription with a capable Service Provider. Consult your system manufacturer and Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit <http://www.intel.com/go/anti-theft>.

No system can provide absolute security under all conditions. Intel® Identity Protection Technology (Intel® IPT) requires an Intel® Identity Protection Technology-enabled system, including a 2nd gen Intel® Core™ processor enabled chipset, firmware and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit <http://ipt.intel.com>.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

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

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

Copyright © 2012-2013, Intel Corporation. All rights reserved.



Contents

1	To-Do Checklist	5
2	Introduction	8
3	Platform Architecture Overview	9

Figures

Figure 1. VIP - Release Notes in Supporting Documentation	7
Figure 2. Platform Architecture and Components	10

Tables

Table 1. To-Do Checklist	5
Table 2. Intel® ME 1.5 MB FW Features and Product SKUs	8



Revision History

Revision Number	Description	Revision Date
0.6	Initial release of the document.	April 2012
0.7	Update to Figure 1 and SKU Matrix table	October 2012
1.0	Revision update only	January 2013

§ §



1 To-Do Checklist

The following checklist is intended to help you get started on using the Intel® Management Engine 1.5 MB Firmware (Intel® ME 1.5 MB FW) release kit.

Table 1. To-Do Checklist

	What You Need To Do	How To Get It Done
<input type="checkbox"/>	Download the latest Intel® ME 1.5 MB FW kit from the Intel Validation Internet Portal (VIP) website	<p>Login to the VIP website at: https://platformsw.intel.com</p> <p>If you know the Kit #, use the box:</p> <div data-bbox="789 747 1218 846"> </div> <p>Otherwise, search for kit by Platform/Product.</p> <p>Note: Engineering releases will be stored under:</p> <div data-bbox="841 951 1182 1012"> </div> <p>This link is located on the left side of the <i>VIP Main Page</i>. Click on this link and search for "ME Firmware 8" to find latest Engineering release kit.</p>
<input type="checkbox"/>	Create a Flash Image for your platform and Program Image onto the SPI Flash devices	<p>Follow the <i>1.5 MB FW Bring Up Guide</i>, which is included with the kit.</p> <p>This document provides step-by-step instructions to create the Flash image. Details are also provided on how to program the image onto Serial Peripheral Interface (SPI) Flash devices and how to perform a quick check on firmware status.</p>
<input type="checkbox"/>	Review the 1.5 MB FW Release Notes ¹	<p>The <i>1.5 MB FW Release Notes</i>¹ document is included with the kit (see Figure 1 for location).</p> <p>This document provides Important Notes as well as Open and Closed Issues for this release. Review these sections for any special instructions required for this release. In addition, these sections identify areas to avoid and workarounds for your platform compliancy and validation testing.</p>
<input type="checkbox"/>	Platform Validation and Compliancy	<p>Login to VIP (https://platformsw.intel.com) and download Intel® ME Compliance and Debug Kit.</p> <p>This kit includes documents, tools and install packages for:</p> <ul style="list-style-type: none"> • Intel® ME Test Suite (see 1.5 MB Compliance Guide) • Intel® Automated Power Switch (Intel® APS) • Intel® ME Debug Tool <p>Follow documents for each component to test platform compliancy.</p>



To-Do Checklist

	What You Need To Do	How To Get It Done
<input type="checkbox"/>	Review Manufacturing Recommendations and Guidelines	<p>The following documents will be available around Beta release timeframe:</p> <ul style="list-style-type: none">• Manufacturing Recommendations for Lynx Point Platforms (available on Intel® Business Portal (IBP) https://businessportal.intel.com)• Manufacturing Advantage Service (MAS) for Lynx Point Platforms (available on Intel® Learning Network (ILN) https://learn.intel.com) <p>In addition, the System Tools User Guide (included with the kit) provides useful information on how to use the following tools in the manufacturing environment: Flash Programming Tool, FWUpdate, MEInfo and MEManuf.</p>

¹ The *1.5 MB FW Release Notes* are included with the release kits on VIP but this document is not in the ".zip" Installation File. The Release Notes can be found in the "Supporting Documentation" section as shown below.

Contact your local Intel representative if you have any questions.



Figure 1. VIP - Release Notes in Supporting Documentation

United States

Worldwide

About Intel

Press Room

Contact Us

Search

Products

Technology & Research

Resource Centers

Support & Downloads

Where to Buy

Intel® Validation Internet Portal

Return to Main Page

Emulate Company

Product Documentation & Other Software

View All Kits

Search Kits

Add/Remove Companies

View VIP License Agreement

Email Notification SignUp & Update

Site Feedback

Manage Home Page Content

Reports

Help

User/Company Request (Sykes)

User/Company Request (AM)

*Requires IBL Access

Manage FAEs

FAE Access

IBL Access

File Queue

Logout

Buy from an Intel® Authorized Distributor >

intel

Authorized Distributor

Software Naming Convention Definition

Release Name:

 Intel® Management Engine Firmware 9.0 SKU 1.5MB and 5MB Alpha 9.0.0.1139

Kit 46262 (Description:

 Intel® ME Firmware 9.0 SKU1.5MB and 5MB,

Posted:

 7/9/2012 4:15:58 PM)

Kit Supported Platforms::

[see list](#)

ADD ALL

 add/remove all kit files to/from download cart

Components

(-) Intel® ME Firmware 9.0 SKU 1.5MB

Package #:

 164849

Release Version:

 9.0.0.1064

Software Version:

 9.0.0.1139v3

(+) Supported Operating Systems

(+) Supported Languages

(-) Supporting Documentation

Add To File Queue

[1.5MB FW Bring Up Guide 9.0.0.1139.pdf](#) (2.13 MB)

Add To File Queue

[1.5MB FW Getting Started Guide.pdf](#) (298.92 KB)

Add To File Queue

[1.5MB FW Release Notes 9 0 0 1139 \(Alpha2\).pdf](#) (608.71 KB)

Add To File Queue

[BIOS_80_Release_Notes.pdf](#) (274.52 KB)

(-) Installation Files

Add To File Queue

[ME9.0_1.5M_9.0.0.1139.zip](#) (114.56 MB)

(+) Intel® ME Firmware 9.0 SKU 5MB

Note: click (+) to expand/collapse entries, click to add file to file queue

§ §

Intel Confidential

7



2 Introduction

This document provides a guide to using the Intel® Management Engine 1.5 MB Firmware (Intel® ME 1.5 MB FW). Important overview details on the platform architecture bring up, compliancy and validation, and manufacturing topics are covered, along with details on where you can find additional information.

The Intel® ME 1.5 MB FW is stored on SPI Flash and executes on the Intel® 8 Series Chipset Family PCH. It enables unique, value-add consumer capability on Intel® 8 Series Chipset Family based platforms. These features are highlighted in the table below:

Table 2. Intel® ME 1.5 MB FW Features and Product SKUs

Intel® 8 Series Series Chipset Family						
Feature	Desktop			Mobile		Details
	H87	Z87	H81	HM87	HM86	
Integrated Clock Control (ICC)	Enhanced ²	Extreme ³	Enhanced ²	Extreme ³	Basic ¹	Controls configuration and settings for platform clocks.
Intel® Anti-Theft Technology (Intel® AT)						Hardware-based security that allows laptops to be disabled if they are lost or stolen.
PAVP						Integrated protected audio and video high definition content.
Identity Protection Technology [®]	N/A	N/A	N/A	N/A	N/A	Intel® Identity Protection Technology (Intel® IPT) provides a simple way for Websites and enterprises to validate that a legitimate user (not malware) is logging in from a trusted PC.
ICC 1 --> Basic Display Clock Bending ICC 2 --> Enhanced Display Clock Bending, Wimax Friendly Clocking ICC 3 --> Extreme Display Clock Bending, Wimax Friendly Clocking, CPU BCLK Overclocking						

For more information regarding the firmware features listed above, please refer to the appropriate Product Requirements Document (PRD), which can be downloaded from the Intel Business Portal (IBP) website at <https://businessportal.intel.com>.

For platform enabling details about Intel® AT Technology, contact your local Intel sales representative, or refer to: <http://www.intel.com/technology/anti-theft/> for general information.

§ §

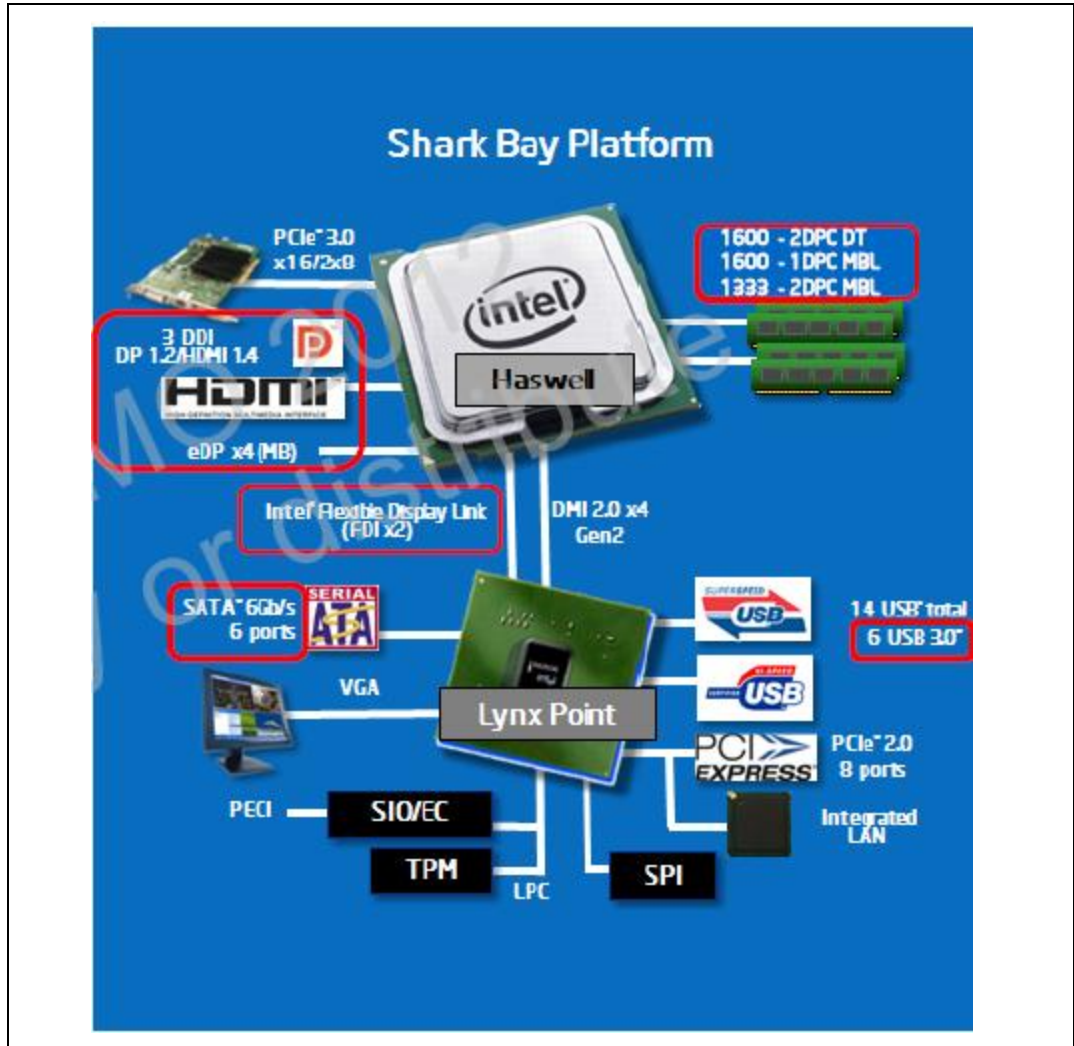


3 Platform Architecture Overview

Platform requirements needed to properly support the Intel® ME 1.5 MB FW include:

- 4th Generation Intel® Core™ processor
- Intel® 8 Series Chipset Family Platform Controller Hub (PCH)
- Hardware design based on Intel Customer Reference Board (CRB) - Haswell Desktop and Mobile CRB.
- The following hardware documents and design files are available on IBP (<https://businessportal.intel.com>):
- Haswell Platform Design Guides
- Haswell Schematics, Layout files and IBIS Models
- 4th Generation Intel® Core™ processor External Design Specification
- Intel® 8 Series Chipset Family PCH External Design Specification

Figure 2. Platform Architecture and Components



§ §