Intel® 6 Series Express Chipset - Intel® Management Engine Firmware 7.1

Changes and Additions to 1.5MB & 5MB Firmware Bring Up Guide and System Tools User Guide 7.0

May 2011

Revision 7.1.13.1088

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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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.

This document contains information on products in the design phase of development.

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.

I2C is a two-wire communications bus/protocol developed by Philips. SMBus is a subset of the I2C bus/protocol and was developed by Intel. Implementations of the I2C bus/protocol may require licenses from various entities, including Philips Electronics N.V. and North American Philips Corporation.

Intel® High Definition Audio requires a system with an appropriate Intel chipset and a motherboard with an appropriate codec and the necessary drivers installed. System sound quality will vary depending on actual implementation, controller, codec, drivers and speakers. For more information about Intel® HD audio, refer to http://www.intel.com/

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security

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

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platformtechnology/intel-amt/

Warning: Altering clock frequency and/or voltage may (i) reduce system stability and useful life of the system and processor; (ii) cause the processor and other system components to fail; (iii) cause reductions in system performance; (iv) cause additional heat or other damage; and (v) affect system data integrity. Intel has not tested, and does not warranty, the operation of the processor beyond its specifications.

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, Intel vPro, Intel Core, 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 © 2008-2011, Intel Corporation. All rights reserved.

Contents

1. Purpose and scope of this document 4
2. Intel® Identity Protection Technology (Intel® IPT) in a nutshell 4

Intel® IPT System Architecture 5

3. Platform preparation for Intel® IPT usage 6
4. FW BRING UP Guide changes and additions to support Intel® DAL 8

4.1 FITC WIZARD 8

4.2 Intel® ME FW Feature configuration 9

5. System Tools User Guide changes and additions to support Intel® DAL 11

5.1 FITC Wizard interface 11

5.2 Intel® MEInfo 12

5.3 Intel® Flash Programming Tool 13

5.4 Intel® ME MANUF 15

1. Purpose and scope of this document

This document explains the changes and additions to Intel® Management Engine (ME) 7.0 documentation that reflect the requirements for Intel® ME 7.1 releases. Changes are relevant to the following documents:

1. FW Bring up Guide (both 1.5MB & 5MB)
2. System Tools User Guide

This document also provides steps required to configure Intel® Dynamic Application Loader (Intel® DAL) parameters thru FITC.

2. Intel® Identity Protection Technology (Intel® IPT) in a nutshell

Intel® Identity Protection Technology (Intel® IPT) is an integrated chipset-based security feature which provides second factor authentication on top of the traditional username and password. Intel® IPT is based on an integration of One-Time-Password (aka OTP) algorithms from OTP Independent Software Vendors (ISVs) into Intel® Manageability Engine (ME).

Intel® Dynamic Application Loading (Intel® DAL) is a new capability added to Intel® Management Engine 7.1 which provides the ability to dynamically run an application on Intel® ME. This is the feature that required for Intel® IPT usage.

Intel® ME Firmware version 7.1 is identical to the general firmware (7.0) with the addition of Intel® DAL capability which enables the usage of Intel® IPT. This firmware is an official POR release.

Intel® IPT System Architecture

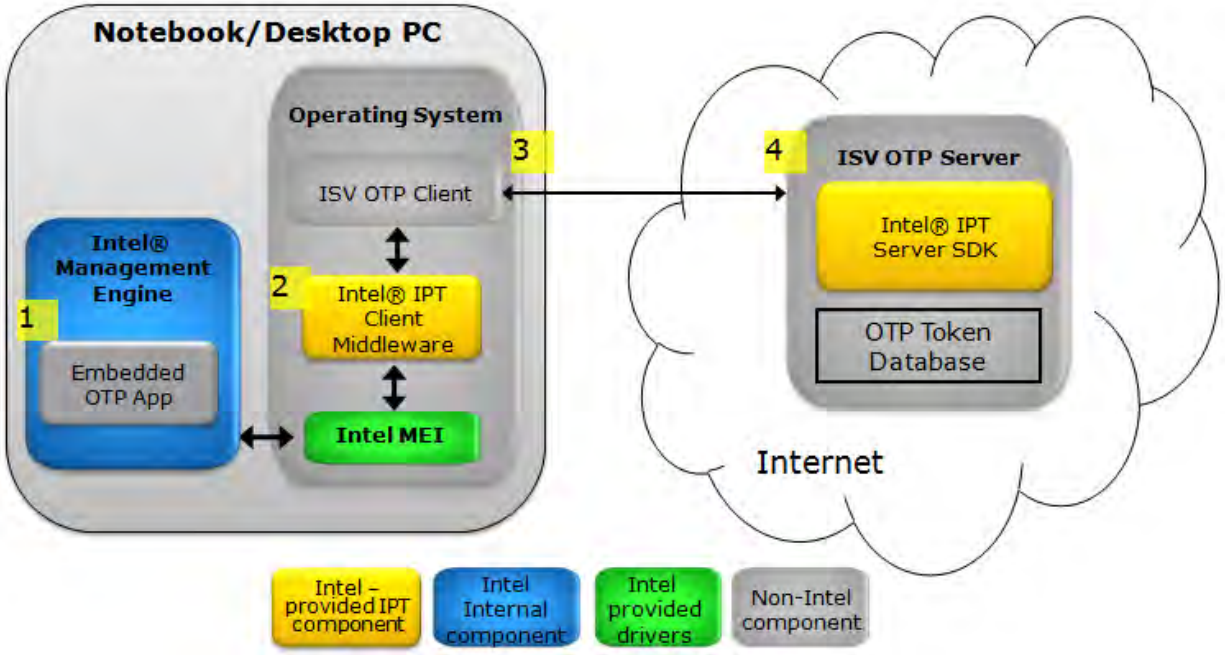


Figure 1. Intel® IPT System Architecture

The figure above shows the client and server components required for the Intel® IPT Technology.

1. Intel® Management Engine (Intel® ME) provides a mechanism to dynamically load and run an Embedded OTP App in the Intel® ME operating environment contained in the chipset (PCH).
2. An ISV uses the APIs exposed by the Intel OTP Client SDK in their OTP Client application to communicate with the Embedded OTP App in Intel® ME via the Intel MEI driver in the OS.
3. The ISV OTP Client communicates with the ISV server on the Internet for OTP Token Activation and OTP Verification.
4. An ISV integrates the Intel OTP Server SDK into their ISV OTP Server for enhancing security during the OTP Token Activation process.

Platforms associated with Intel® IPT

Intel® IPT will be available only with the new 2nd generation Intel® Core™, Intel® Core™ vPro™ and Intel® Xeon® CPUs, on the following chipset SKUs (1.5MB and 5MB).

Huron River 2011 Notebook chipset SKUs:
QM67 (5MB), QS67 (1.5MB & 5MB), HM67 (1.5MB & 5MB), HM65 (1.5MB & 5MB), UM67 (1.5MB & 5MB)

Sugar Bay 2011 Desktop chipset SKUs:
Q67 (5MB), Q65 (5MB), B65 (5MB), H67 (1.5MB & 5MB), H61 (1.5MB), Z67 (1.5MB), Z68 (1.5MB).

Intel® IPT supported operating systems

Windows XP (32 bit)
Windows Vista (32 bit & 64 bit)
Windows 7 (32 bit & 64 bit)

3. Platform preparation for Intel® IPT usage

No BIOS or HW changes are required for Intel® IPT functionality.
On top of Intel® Management Engine being turned on, there is one Intel® IPT- specific parameter update required in the Intel® ME image – unique ODM ID using FITC tool.

FITC – 2 parameters are related to Intel® IPT:

1. ODM ID used by Intel Service. This parameter is for tracking which OEM platforms (brand-wise) Intel® IPT Technology is being used on. It is required for platform identification between the OEM and the ISV (e.g. potential for business agreements between OEM & ISV).
   Note: This parameter will be provided by Intel to the OEM.

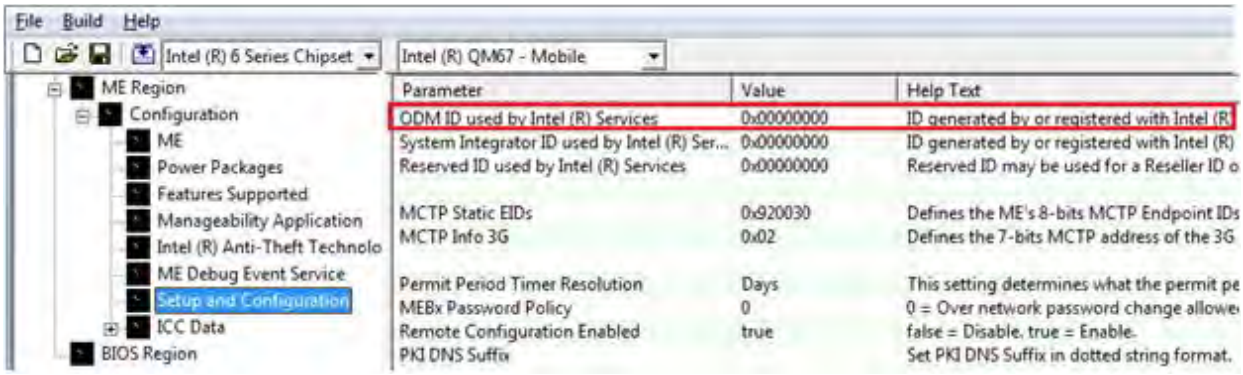


Figure 1: How to configure ODM ID

2. "Intel ® DAL Permanently Disabled?" This is the parameter that configures Intel® Dynamic Application Loader (Intel® DAL) permanent state. No configuration is needed as it is enabled by default (set to "No").
   Located at: ME Region → Configuration → Features Supported (see Figure 2)

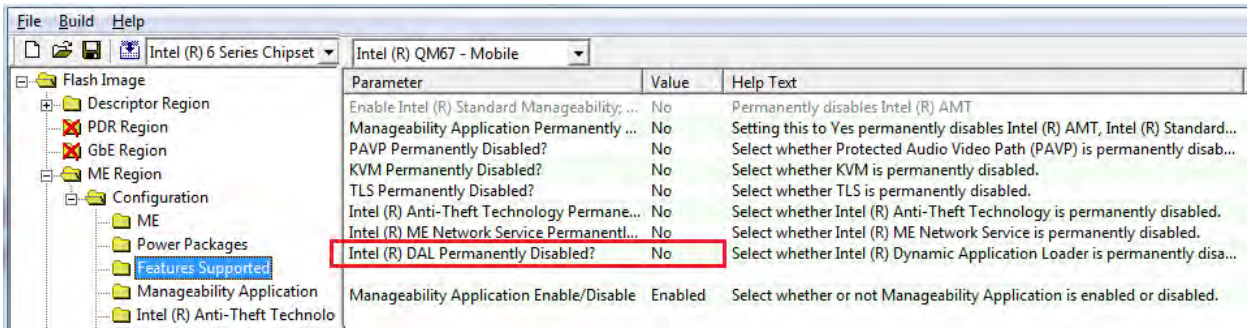


Figure 2: How to enable Intel® DAL

4. FW BRING UP Guide changes and additions to support Intel® DAL

4.1 FITC WIZARD

The following change refers to chapter 2.2 - Step-by-Step Guide to Build SPI Flash Image with FITC Wizard Interface.

Table 2-5:

Table 2-5. FITC Wizard - Intel ME Application Permanent Disable

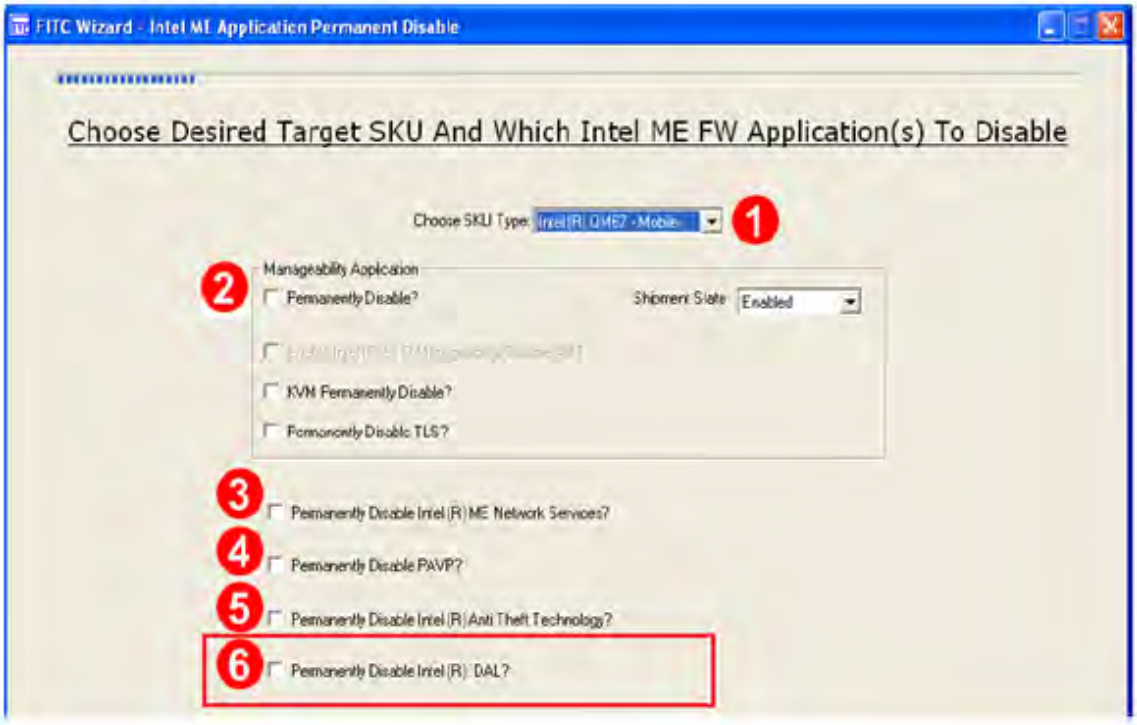
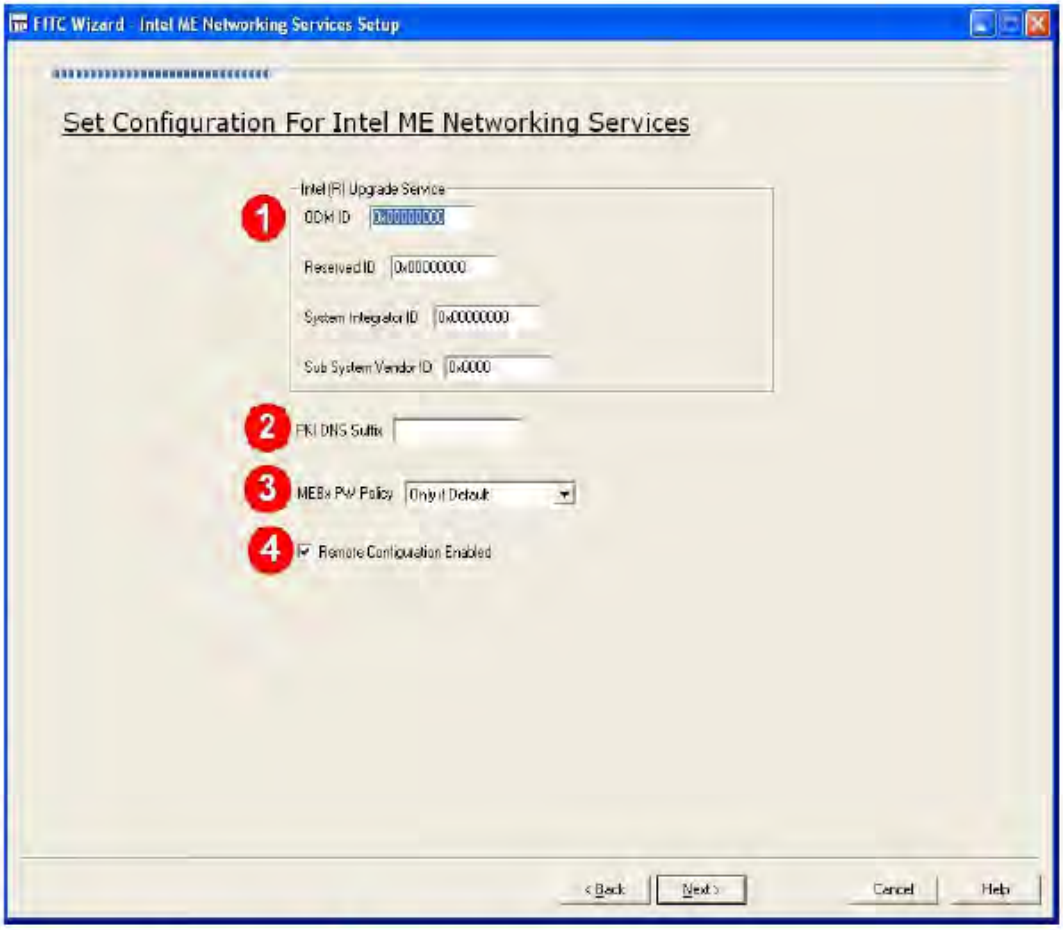
#	CRB Setting	Settings for All Platforms
		
6	Unchecked	Availability of Intel® Dynamic Application Loader (Intel® DAL) feature is dependent on the SKU Type selected in Step 1. If this feature is not grayed out, then you have the option to enable /disable using the pull down menu option.

Table 2-8:

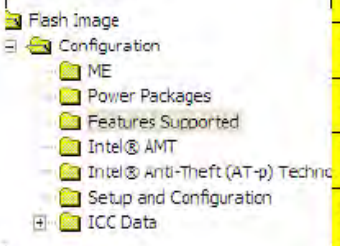
Table 2-8. FITC Wizard - Intel ME Networking Services Setup

#	CRB Setting	Settings for All Platforms
		
1	ODM ID: **0x00000000** Reserved ID: **0x00000000** System Integrator ID: **0x00000000** Sub System Vendor ID **0x0000**	These fields are used by Intel® Services. Intel® Identity Protection Technology (Intel® IPT) use ODM ID field only (for platform identification between the OEM and the ISV) If enabling Intel® Upgrade Service, refer the MTP User Guide that is available after registration for detail on how to set this field. Registration and login is available at: http://upgrades.intel.com

4.2 Intel® ME FW Feature configuration

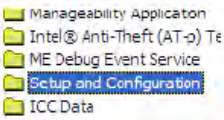
The following addition refers to chapter 3.6 – Intel® ME Firmware Feature configuration (Table 3-25)

Table 3-25. Flash Image | ME Region | Configuration | Features Supported

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Features Supported** • Set the parameters in the **Features Supported** section as shown 	**Yellow means custom settings may be required.**		
	Enable Intel® Standard Manageability; Disable Intel® AMT	No	***Note:*** Setting any of these options to 'Yes' will permanently disable that specific feature. Once the feature is disabled in this manner only re-flashing the ME region can re-enable the feature. Fields are read only if the feature is not supported by respective PCH SKU selected by PCH SKU pull down (see Section 3.5).
	Intel® Manageability Application Permanently Disabled?	No	
	PAVP Permanently Disabled	No	
	KVM Permanently Disabled?	No	
	TLS Permanently Disabled?	No	
	Intel® Anti-Theft Technology Permanently disabled	No	
	Intel® ME Network Service Permanently disabled	No	
	Intel® DAL Permanently disabled	No	
	Intel® Manageability Application Enable/ Disable	Enabled	This setting determines shipping state of the Manageability Application in the base image. **Setting Options:** Enabled (Full Manageabilty) **Default** Disabled (No Manageability)

The following change refers to chapter 3.6 – Intel® ME FW Feature Configuration (Table 3-29)

Table 3-29. Flash Image | ME Region | Configuration | Setup and Configuration

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Setup and Configuration** • Set the parameters in the **Setup and Configuration** section as shown 	**Yellow means custom settings may be required.**		
	ODM ID used by Intel(R) ~~Upgrade~~ Services	0x00000000	Used by Intel® Upgrade Service, Intel® AT and Intel® IPT. If enabling Intel® Upgrade Service, refer the MTP User Guide that is available after registration for detail on how to set this field. The OEM can find their value by logging on to **http://upgrades.intel.com**
	System Integrator ID used by Intel(R) ~~Upgrade~~ Service	0x00000000	Used ONLY by Intel® Upgrade Service. If enabling Intel® Upgrade Service, refer the MTP User Guide that is available after registration for detail on how to set this field. Registration and login is available at http://upgrades.intel.com
	Reserved ID used by Intel(R) ~~Upgrade~~ Service	0x00000000	Used ONLY by Intel® Upgrade Service. If enabling Intel® Upgrade Service, refer the MTP User Guide that is available after registration for detail on how to set this field. Registration and login is available at http://upgrades.intel.com

5. System Tools User Guide changes and additions to support Intel® DAL

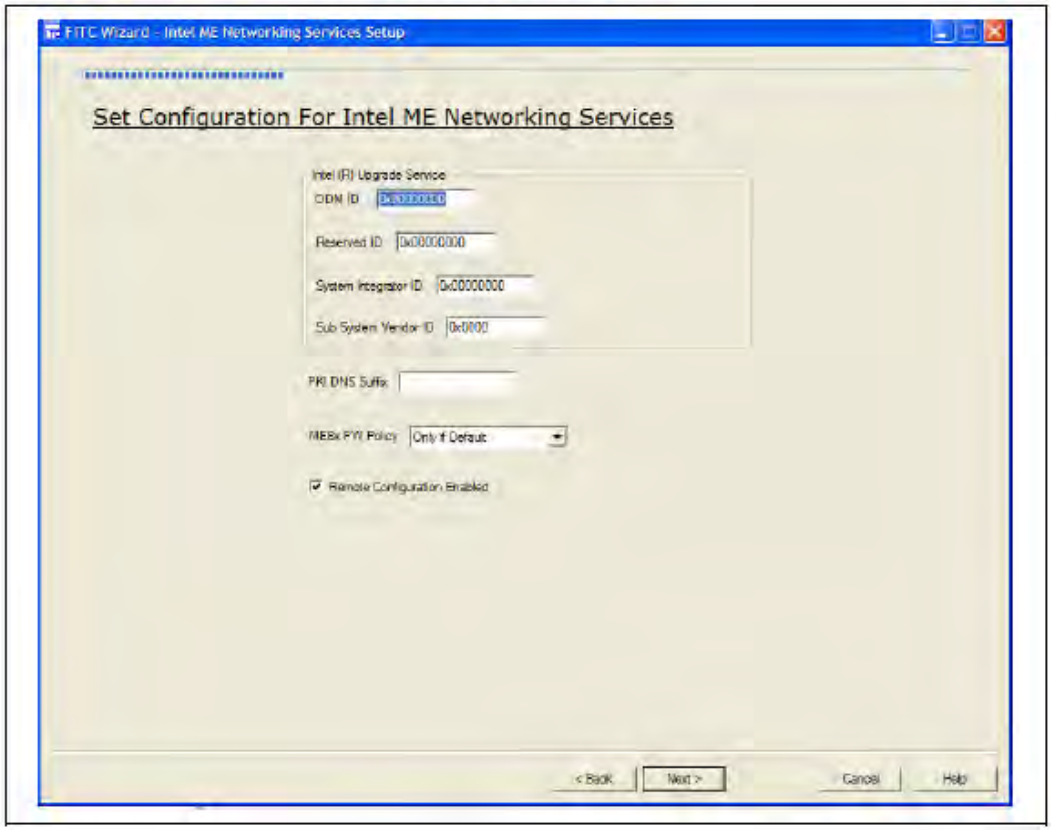
5.1 FITC Wizard interface

The following change refers to Chapter 3.5 – FITC Wizard Interface

For your reference, this is the figure and explanation as it appears in the System Tools User Guide:

3.5.2.9 Intel® ME Networking Services Setup Screen

Figure 9: Intel® ME Networking Services Setup Screen

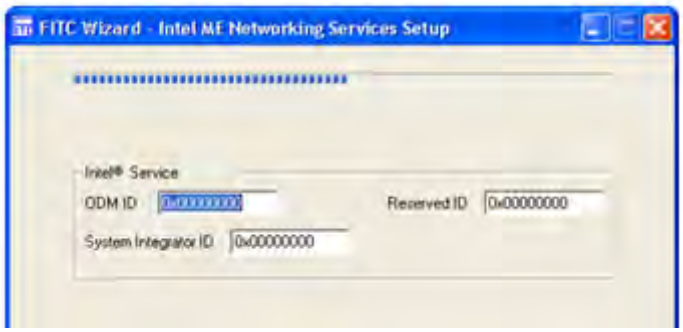


This screen contains the following options for configuring Networking Services parameters:

- Intel Upgrade Service Section:
  - ODM ID – ID generated by or registered with Intel® Upgrade web servers in order to identify the ODM/Board builder. First of three IDs stored in flash and accessible through Intel® MEI interface.
  - System Integrator ID – ID generated by or registered with Intel® Upgrade web servers in order to identify the System Integrator. Second of three IDs stored in flash and accessible through Intel® MEI interface.

- Reserved ID – May be used as a reseller ID or other Intel® service IDs in the future

Changes required for Intel® IPT:



This screen contains the following options for configuring Networking Services parameters:

- Intel Services Section:
  - ODM ID – ID generated by or registered with Intel® Upgrade web servers and/or Intel® IPT in order to identify the ODM/Board builder. First of three IDs stored in flash and accessible through Intel® MEI interface.
  - System Integrator ID – ID generated by or registered with Intel® Upgrade web servers in order to identify the System Integrator. Second of three IDs stored in flash and accessible through Intel® MEI interface.
  - Reserved ID – May be used as a reseller ID or other Intel® service IDs in the future

5.2 Intel® MEInfo

The following addition refers to Chapter 6 – Intel® MEInfo, Table 20 - List of Components for which Version Information is retrieved

Following is an additional component to be added to the table:

Feature Name	Feature Data Source (ME Kernel/AMT/ SW/Other)	Consumer SKU	Corporate SKU	Specific Feature Dependency	Field Value
Intel® ME Dynamic Application Loader (DAL)	ME Kernel	X	X	N/A	Present/Enabled Present/Disabled NotPresent

5.3 Intel® Flash Programming Tool

The following functions were added to FPT (DOS and Windows* versions) to support Intel® DAL configuration (note that the examples below are with FPTW but also applicable to DOS FPT):

1. Retrieve “ODM ID” value.
   FPTW.exe -r "ODM ID used by Intel (R) Services"
   Notes: This value is returned hashed. If this parameter is not set (remains 0x00000000 as default), the command above will return an error.

2. Set Intel® Dynamic Application Loader (Intel® DAL) capability (permanent bit) thru the FOV mechanism:
   FPTW.exe -u -n OEMSkuRule -v HEX_VAL
   Where HEX_VAL is a hexadecimal value which represents features availability.
   Intel® DAL represented in bit 20 (1-enabled, 0-disabled)
   For more details refer to “System Tools User Guide” document – Appendix A Fixed Offset Variables (relevant part from Appendix A added below).

3. Retrieve Intel® DAL capability (permanent bit):
   FPTW.exe –r “Intel(R) DAL Permanently Disabled?”
   “Yes / 00” – Intel® DAL permanently disabled
   “No / 01”- Intel® DAL permanently enabled

4. Retrieve Intel® DAL shipment state value:
   FPTW.exe –r "Intel(R) DAL Enabled/Disabled”

5. Set Intel® DAL shipment state value thru the FOV mechanism
   FPTW.exe -u -n FeatureShipState -v HEX_VAL
   Where HEX_VAL is a hexadecimal value which represents features availability.
   Intel® DAL represented in bit 20 (1-enabled, 0-disabled)

The following addition refers to Appendix A Fixed Offset Variables

The following table refers to the FOV “OEMSkuRule” which provides the ability to permanently Disable/Enable Intel® Dynamic Application Loader (in addition to other supported features)

<table>
<tr><th>Fixed Offset Name</th><th>FPT ID</th><th>Fixed Offset ID</th><th>Description</th><th>Data Length (in Bytes)</th><th>Expected Value</th></tr>
<tr>
<td>OEM Permanent Disable

FOV value: OEMSkuRule</td>
<td>7</td>
<td>0x000A</td>
<td>UINT32 (little endian) value. This controls what features are permanently disabled by OEM
Notes:
User must set all non-reserved bits to the value they want. There is NO ability to change features one at a time. This FOV sets OEM Permanent Disable for ALL features.
This will not enable functionality that is not capable of working in the target hardware SKU. Please see the respective Firmware Bring-up Guide for a list of what features are capable with what firmware bundle and Hardware SKU of Intel 6 Series Chipset.
Examples:
• Intel® Q67 with Intel® AMT, KVM and PAVP 1.5 and TLS enabled: Bits: 0,2, 12, 18,21 set to ‘1’ (0x241005)
• Intel® QM67 with disabling Intel® AMT, PAVP 1.5 enabled: Bits: 12 set to ‘1’ (0x1000)
• Intel® HM67 with PAVP 1.5 and KVM and TLS disabled: Bits: 12, 18, 21 (0x241000)</td>
<td>4</td>
<td>Feature Capable: 1
Feature Permanently disabled: 0

<table>
<tr><th>Bit</th><th>Description</th><th>Notes</th></tr>
<tr><td>31:22</td><td>Reserved</td><td></td></tr>
<tr><td>21</td><td>TLS</td><td></td></tr>
<tr><td>20</td><td>Intel® DAL</td><td>3</td></tr>
<tr><td>19</td><td>Reserved</td><td></td></tr>
<tr><td>18</td><td>KVM</td><td>2</td></tr>
<tr><td>17</td><td>Reserved</td><td></td></tr>
<tr><td>16</td><td>HAP</td><td></td></tr>
<tr><td>15:13</td><td>Reserved</td><td></td></tr>
<tr><td>12</td><td>PAVP</td><td></td></tr>
<tr><td>11:6</td><td>Reserved</td><td></td></tr>
<tr><td>5</td><td>Intel® AT</td><td></td></tr>
<tr><td>4:3</td><td>Reserved</td><td></td></tr>
<tr><td>2</td><td>Manageability and Security Application</td><td>1</td></tr>
<tr><td>1</td><td>Reserved</td><td></td></tr>
<tr><td>0</td><td>Manageability Full</td><td>1</td></tr>
</table>
1. For corporate SKUs (Intel® Q67, Intel® QM67, Intel® QS67) bits 0 and 2 need to be both set to ‘1’ to allow for Intel® AMT to work.
2. KVM (bit 18) should only be set to ‘1’ when Manageability Application (bit 2) is set to ‘1’. If using a Corporate SKU, then Manageability Full (bit 0) must also be set to ‘1’.
3. Intel® Dynamic Application Loader (Intel® DAL) available only on Intel® ME FW 7.1 (bit 20). Set bit to ‘1’ to enable Intel® DAL or ‘0’ to disable Intel® DAL.
Reserved bits should be set to ‘0’.</td>
</tr>
</table>

<table>
<tr><th>Fixed Offset Name</th><th>FPT ID</th><th>Fixed Offset ID</th><th>Description</th><th>Data Length (in Bytes)</th><th>Expected Value</th></tr>
<tr>
<td>Feature Shipment Time State

FOV Value: FeatureShipState</td>
<td>8</td>
<td>0x000B</td>
<td>UINT32 (little endian) value. This controls what features are enabled or disabled. These features may be enabled /disabled by mechanisms such as MEBx or provisioning. This setting is only relevant for features NOT permanently disabled by the OEM Permanent Disable.
Notes:
User must set all nonreserved bits to the value they want. There is NO ability to change features one at a time. This will not enable functionality that is not capable of working in the target hardware SKU. Please see the respective Firmware Bring-up Guide for a list of what features are capable with what firmware bundle and Hardware SKU of Intel 6 Series Chipset.
Examples:
• Intel® Q67 with Manageability Application, ship enabled: Bit: 2 set to ‘1’ (0x4)
• Intel® QM67 with disabling Manageability Application, Bit: 2 none set to ‘0’ (0x4)</td>
<td>4</td>
<td>Feature Enabled: 1
Feature Disabled: 0
Bit Description Notes

<table>
<tr><th>Bit</th><th>Description</th><th>Notes</th></tr>
<tr><td>31:21</td><td>Reserved</td><td></td></tr>
<tr><td>20</td><td>Intel® DAL</td><td>See below</td></tr>
<tr><td>19:3</td><td>Reserved</td><td></td></tr>
<tr><td>2</td><td>Manageability Full</td><td></td></tr>
<tr><td>1:0</td><td>Reserved</td><td></td></tr>
</table>

Intel® Dynamic Application Loader (Intel® DAL) available only on ME FW 7.1 (bit 20). Set bit to ‘1’ to enabled Intel® DAL or ‘0’ to disable Intel® DAL.

All other bits are reserved. Reserved bits should be set to 0.</td>
</tr>
</table>

5.4 Intel® ME MANUF

The following additions refer to Chapter 5 – MEManuf and MEManufWin.
The **MEMANUF.cfg** file includes all the test configurations for `MEMANUF -EOL` check.
Intel® DAL will have the following tests:

- SubTestName=”Intel(R) DAL Permanently Disabled?", ReqVal=<Yes | No> or <00 | 01>
  (Yes / 00 – Intel® DAL is permanently disabled. No / 01 Intel® DAL is permanently enabled)

- SubTestName="Intel(R) DAL Enabled/Disabled", ReqVal= <Enabled | Disabled> or <01 | 00> (00 – Intel® DAL shipment state is disabled. 01 – Intel® DAL shipment state is enabled)

- SubTestName="ODM ID used by Intel (R) Services", ReqVal=HEX_VAL (HEX_VAL is a hashed hex decimal value of the ODM ID)