

Intel® Platform Trust Enabler

Product Guide

July 2016

Revision 2.2
333845-003



Revision History

Revision	Date	Comments
2.2	July 1, 2016	Intel® Platform Trust Enabler, Version 2.1. - Minor edits.
2.1	June 24, 2016	Intel® Platform Trust Enabler, Version 2.1.
2.0	January 29, 2016	Intel® Platform Trust Enabler, Version 2.0.
1.0	May 11, 2015	Initial release (Intel Public).



Contents

1.0	Introduction	5
1.1	Overview	5
1.2	What is Intel® Platform Trust Enabler?	5
1.3	Requirements.....	5
1.4	Solution Architecture.....	6
1.5	Deployment Topology.....	6
1.6	Server Execution Flow	7
2.0	Installation	7
2.1	PXE Server Configuration	8
2.1.1	Reference Screen Shots for PXE Configuration	8
3.0	User Guide	9
4.0	OEM Support Matrix	12
5.0	Tested Scenarios.....	12
6.0	Appendix.....	13
6.1	Prerequisites.....	13
6.1.1	Prerequisite for Supermicro.....	13
6.1.2	Prerequisite for Dell	13
6.1.3	Prerequisite for Quanta	13
6.2	Steps to Add Support for Additional OEMs	14



NOTE: *This page intentionally left blank.*



1.0 Introduction

This product automates Intel® Trusted Execution Technology (Intel® TXT) and Trusted Platform Modules (TPM 1.2) activation. It is assumed that the user is familiar with Linux® (Ubuntu™) administration.

1.1 Overview

Computing platforms supporting Intel® TXT are supplied to end users with Intel® TXT in a disabled state. Intel® TXT-enabling ("opting-in") must be a conscious step performed by the IT department or end user.

The high level steps to provision the platform are as follows:

- **Enable the TPM** — This is a relatively simple step, but it is platform specific. That is, different manufacturers have different BIOS Setup menus, and thus the control to enable and activate the TPM may be in different locations (such as Security tab, Processor tab, Advanced Configuration tab, and so on). This step usually requires restarting the platform so the TPM can be properly started.
- **Enable Intel® TXT** — This also is a relatively simple step, and is also platform specific. In the BIOS **Setup** menu, find the Intel® Trusted Execution Technology control and set it to **Enabled**. Also make sure that virtualization is enabled (VMX and VT-d). Save the settings and let the platform power cycle to enable Intel® TXT.

1.2 What is Intel® Platform Trust Enabler?

Intel® Platform Trust Enabler (Intel® PTE) is a PXE-based solution that automates the TXT/TPM activation. Intel® PTE 2.1 is a free software framework that has flexibility to support additional OEM's. Customers are encouraged to modify the code to support additional OEM's.

What Intel® PTE 2.1 solves:

- Automates the TXT/TPM Activation in BIOS console.

What Intel® PTE 2.1 does not solve:

- TPM 1.2 hardware provisioning.
- Discovery of TXT/TPM supported hardware in given DC.
- TXT Provisioning/Launch in Linux distribution.
- Intel® Cloud Integrity Technology ATAG Provisioning in TPM 1.2.

1.3 Requirements

Following are the requirements for Intel® PTE 2.1:

- BMC IP configured Target Intel® TXT Node, which should be in DC powered off state.
- Ubuntu 12.04.05 VM to install Intel® PTE 2.1 binary file.
- OEM SYSCFG tools.
- PXE Server with NFS share configured.
- System Admin with Linux Expertise.

1.4 Solution Architecture

Figure 1 shows the high-level architecture for Intel® PTE 2.1.

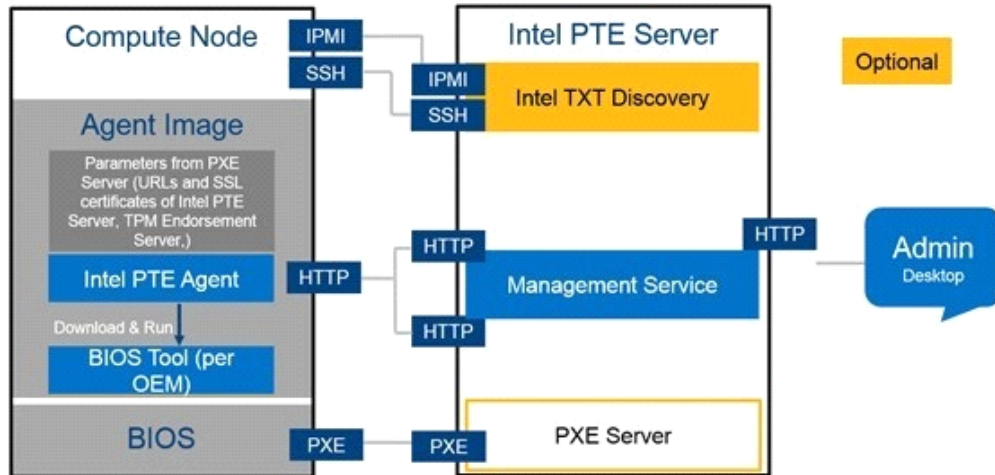


Figure 1. High-Level Solution Architecture (Version 2.1)

1.5 Deployment Topology

Figure 2 shows the deployment topology.

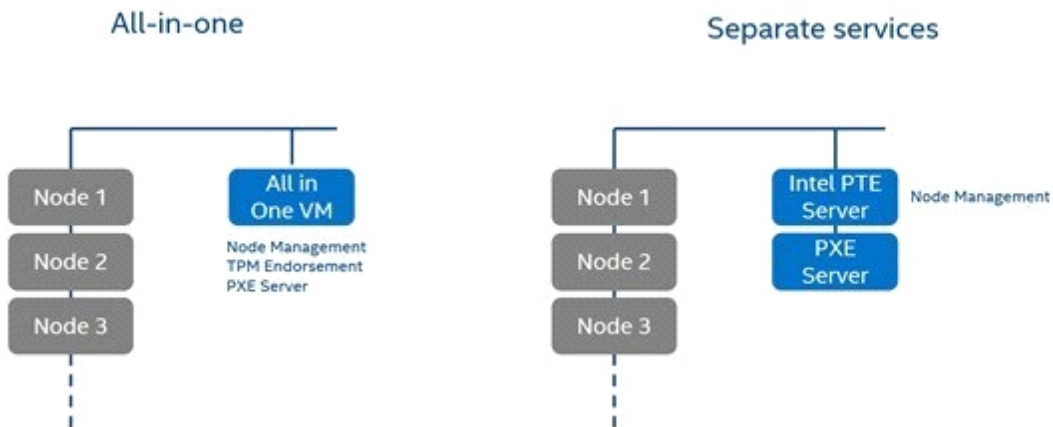


Figure 2. Deployment Architecture

Notes:

- The deployment topology is validated in a IPXE environment.
- Intel® Platform Trust Enabler Appliance is shipped as a binary file and validated in Ubuntu 12.04.05.

1.6 Server Execution Flow

Figure 3 shows the high-level execution flow.

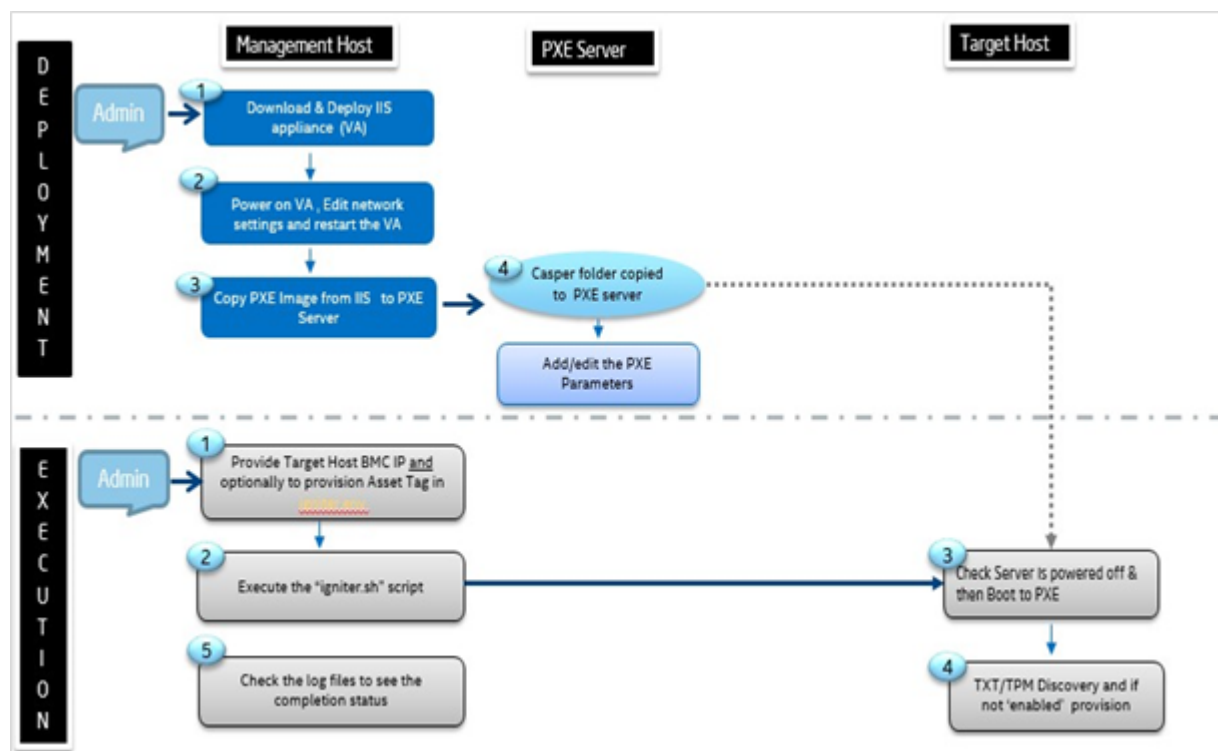


Figure 3. Deployment and Execution High-Level Flow

2.0 Installation

To install Intel® PTE 2.1, execute the following steps:

1. Download and install *pte-2.1-SNAPSHOT.bin* in plain vanilla Ubuntu 12.04.05 VM.

```
$ ./pte-2.1-SNAPSHOT.bin
# default credentials = admin/password
$ pte password <admin password> --permissions *:*
```

2. Copy the created PXE image to the PXE server.

3. Upload the appropriate OEM BIOS tools to the PTE OEM path. For example:

```
/opt/pte/software/oem/dell/2.0/tools/
```

4. Once the tools are in the corresponding path, change the owner to *pte* user. For example:

```
$ chown -R pte:pte /opt/pte/software/oem/dell/2.0/tools/*.*
```

5. Connect to the PTE2 Portal.

6. Add the BMC address of the Target Node.

7. Check the desired actions and click the **Run the Actions** button.



2.1 PXE Server Configuration

To configure the PXE Server, follow these steps:

1. Copy the *casper* folder from the Intel® PTE 2.1 appliance (path = */mnt/*) to the PXE NFS share. For more details on how to setup the PXE server, see <http://ipxe.org/docs>.
2. Ensure there is no network issue between Intel® PTE server and PXE servers. Check by mounting the NFS drive of the PXE server.

2.1.1 Reference Screen Shots for PXE Configuration

Sample *menu.ipxe* file:

```
:iistestkn
echo "#####"
echo "# PXEBOOT HAS STARTED... #"
echo "#####"
sleep 2
echo mac.....: ${mac}
echo ip.....: ${ip}
echo netmask.....: ${netmask}
echo gateway.....: ${gateway}
echo dns.....: ${dns}
echo dhcp-server.....: ${dhcp-server}
echo syslog.....: ${syslog}
echo filename.....: ${filename}
echo next-server.....: ${next-server}
echo hostname.....: ${hostname}
echo uuid.....: ${uuid}
echo serial.....: ${serial}
echo Loading vmlinuz...
kernel nfs://${nfs-server}:${nfs-root2}/user/casper/vmlinuz echo Loading initrd...
sleep 3
initrd nfs://${nfs-server}:${nfs-root2}/user/casper/initrd.gz
sleep 3
echo "Loading variables for Ignition server..."
imgargs vmlinuz root=/dev/nfs boot=casper netboot=nfs nfsroot=${nfs-server}:${nfs-root}/user
locale=en_US.UTF-8 PTE_SERVER=http://192.168.19.117/v1 BIOS_PASSWORD='P@ssw0rd'
sleep 5
boot || goto failed
goto start
```

Sample *boot.ipxe.cfg* file:

```
#!ipxe
# NFS server used for menu files and other things
# must be specified as IP, as some distros don't do proper name resolution set nfs-server
192.168.19.20
set nfs-root /home/exports set nfs-root2 /home/exports2
# Base URL used to resolve most other resources
# Should always end with a slash
#set boot-url http://boot.smidsrod.lan/ set boot-url http://192.168.19.20/nfsshare
# REQUIRED: Absolute URL to the menu script, used by boot.ipxe
# and commonly used at the end of simple override scripts
# in ${boot-dir}.
set menu-url ${boot-url}/menu.ipxe
```




3.0 User Guide

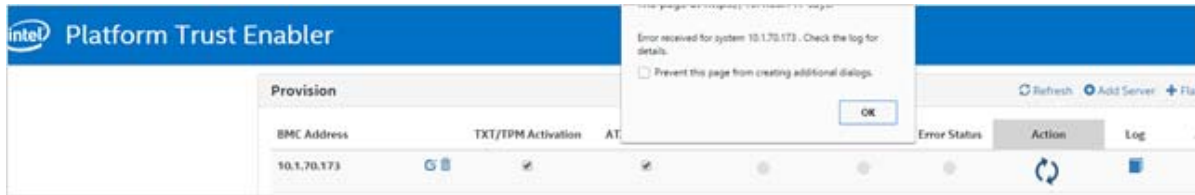
1. Connect the portal using https service.
`https://<pteip>/index.html`
2. Sign in to the Platform Trust Enabler. The default credentials are **admin** and **password**. (The credentials made with the `pte password` command.)

3. Select **Portal > Login > Add Server** and enter the BMC Address.

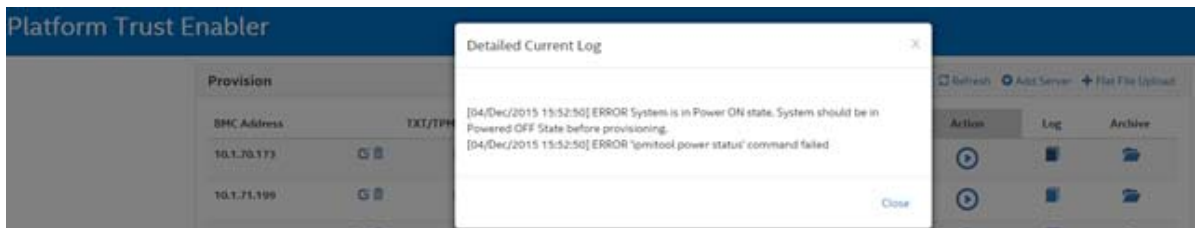
4. Select **Portal > Login > Dashboard**, check the desired actions, and click **Action**.

Note: Once the **Action** button is pressed, the spinning arrow indicates that job execution is live in background.

Note: The Intel® Cloud Integrity Technology instance should be up and running to provision the ATAG, and ATAG variables should be defined as PXE variables.



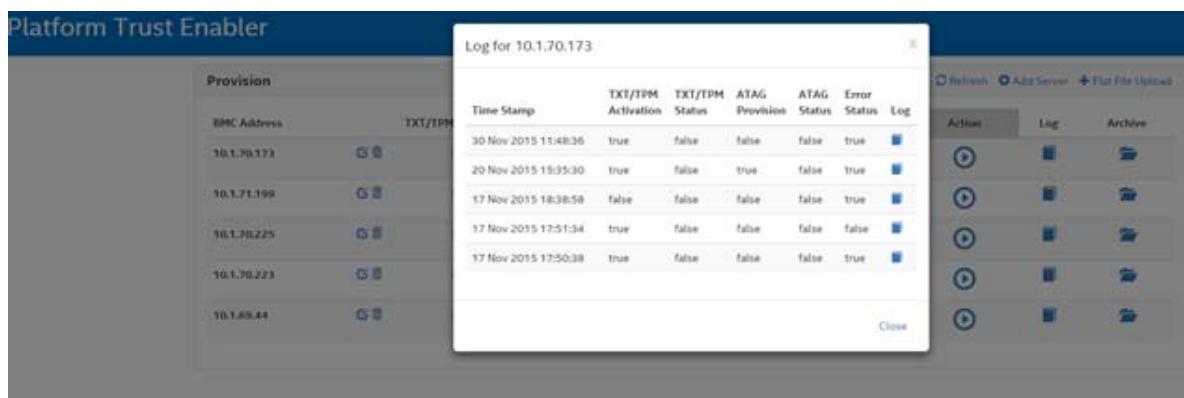
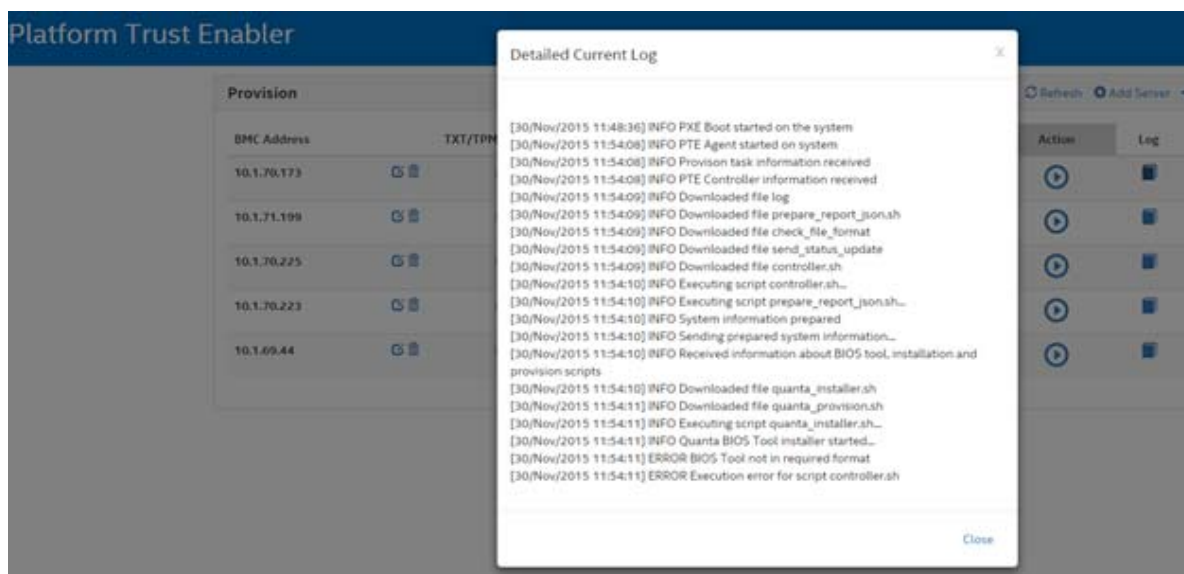
5. Power off the host before initiating action through PTE.



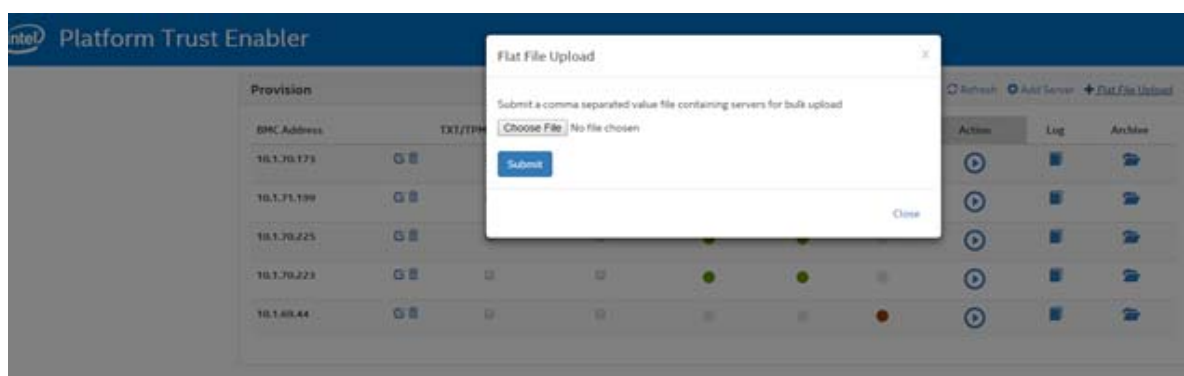
6. Dashboard:

- **TXT/TPM Status** and **ATAG Status** buttons show the status of the Job Execution initiated through PTE. Green depicts that the job is complete.
- **Error Status** button displays if there is any error/warning encountered in the job initiated by PTE.
- **Log** details the current execution logs initiated through PTE.
- **Archive** details the history of executed logs initiated through PTE instance.

BMC Address	TXT/TPM Activation	ATAG Provision	TXT/TPM Status	ATAG Status	Error Status	Action	Log	Archive
10.1.70.173								
10.1.71.199								
10.1.70.225								
10.1.70.223								
10.1.69.44								



7. Feature: Flat file Upload.





Note: BMC IP and credentials should be separated by commas, as shown below, and save as *sample.csv*.

```
1 10.1.68.232,ADMIN,ADMIN
2 21.7.1.2,root,P@ssw0rd
```

4.0 OEM Support Matrix

OEMs	Platform Name	Supported BIOS Version	Supported and Tested BIOS Tool Version
Dell	PowerEdge R730	2.1.6	OMSA (racadm) v7.4 and Dtk v4.3
Intel PCSD	S2600WT2	SE5C610.86B.01.01.1008	Syscfg_V13_1_Build14_AIIOS
SuperMicro	X1-DRL-i	American Megatrends Inc. v1.0	Supermicro Update Manager v1.6.0. and SUM driver source code (check appendix 6.1 step 3)
SuperMicro	X10SLH-F/X10SLM+-F	American Megatrends Inc. v3.0	Supermicro Update Manager v1.6.0. and SUM driver source code (check appendix 6.1 step 3)
Quanta	S100-X1S1N	S1N_3A13	SCELNx64_v5.02.1092
HP	ProLiant DL360 Gen9	P89 07/20/2015	HP Scripting Tools Linux RPM Packaging v10.30, HP Scripting Toolkit Linux v10.30

5.0 Tested Scenarios

Out of the Box Configuration:

- TPM 1.2/Intel® TXT activation.

TPM	TXT	TXT/TPM Activation Requirement
Off	Off	Yes
On	Off	Yes
On	On	Yes
Load Default (OEM Configuration)		Yes



6.0 Appendix

6.1 Prerequisites

6.1.1 Prerequisite for Supermicro

1. To work with the SYSCFG tools of Supermicro, a SUM (Supermicro Update Manager) tool license is required. You can buy licenses through a reseller or directly through Supermicro at:

sales@Supermicro.com

2. The MAC address of each server needs to be provided to Supermicro in order to generate the activation key of the SUM tool.
3. In addition to the SUM tool you will need to request the SUM driver directly from SUM support at:
mgmtsw@supermicro.com

The recommended version and tested on this version of PTE is *sum_driver_V1.6.0_20151119.tar*.

6.1.2 Prerequisite for Dell

1. The Lifecycle Controller (CSIOR) must be enabled in the BIOS.
2. Make sure you have the following files:

- *srvadmin-omilcore*.deb*
- *srvadmin-deng*.deb*
- *srvadmin-hapi*.deb*
- *srvadmin-isvc*.deb*
- *srvadmin-smcommon*.deb*
- *srvadmin-storelib-sysfs*.deb*
- *srvadmin-storelib*.deb*
- *raidcfg*.deb*
- *srvadmin-racadm4*.deb*
- *srvadmin-racadm5*.deb*
- *srvadmin-idracadm_*.deb*
- *srvadmin-idracadm7*.deb*
- *syscfg*.deb*
- *dtk-scripts*.deb*

3. Files can be found in:

- <http://linux.dell.com/repo/community/ubuntu/pool/precise/openmanage/740/OMSA/all/>
- <http://linux.dell.com/repo/community/ubuntu/pool/precise/openmanage/740/OMSA/amd64/>

6.1.3 Prerequisite for Quanta

Contact Quanta's support team to get the SYSCFG tools. Refer to the OEM support matrix for tested versions.



6.2 Steps to Add Support for Additional OEMs

Note: To write their own scripts, users must have knowledge of existing BIOS tool installation to write their own scripts.

1. On compute node, find the Manufacturer (OEM) name displayed using the **dmidecode** command. The following script could display the OEM name:

```
dmidecode > /root/ignition/dmi
OEM=$(dmidecode | grep -n "System Information" | cut -d : -f 1)
OEM=$((OEM + 1))
OEM=$(sed "${OEM}!d" /root/ignition/dmi | cut -d : -f 2 | sed -e 's/^ *//' -e 's/ *$//')
echo $OEM
```

2. After installing PTE server, add the entry for above displayed OEM name in the */opt/pte/configuration/pte_version.xml* file. You must also choose the directory name to store the scripts and tools for the OEM.

```
<oem name="Dell Inc.">
  <directory>dell</directory>
</oem>
```

3. On the PTE server, in the */opt/pte/configuration/oem_version.xml* file, add the directory name chosen above along with a version. This allows activating a particular version of scripts/tools in case there are multiple versions of scripts/tools for an OEM. Currently, only once version of tool/scripts is supported for all OEMs, so the default version is 2.0 for all OEMs.

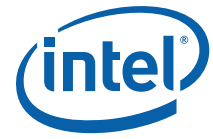
```
<oem name="dell">
  <version>2.0</version>
</oem>
```

4. Prepare the BIOS tool installation script with name *dell_installer.sh* and provision script with name *dell_provision.sh*.
5. On the PTE server, add the installation and provision scripts (*dell_installer.sh* and *dell_provision.sh*, respectively) as follows:

```
/opt/pte/software/oem/dell/2.0/scripts/dell_installer.sh
/opt/pte/software/oem/dell/2.0/scripts/dell_provision.sh
```

6. Add the BIOS tool in the following location:

```
/opt/pte/software/oem/dell/2.0/tools/
```



NOTE: *This page intentionally left blank.*



LEGAL

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 contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors which may cause deviations from published specifications.

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 and 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.

© 2015-2016 Intel Corporation.