Intel® Platform Trust Enabler

Product Guide

January 2016

Revision 2.0
333845-001

Revision History

Revision	Date	Comments
2.0	January 29, 2016	Major edits to all sections.
1.0	May 11, 2015	Initial release (Intel Public).

Contents

NOTE: This page intentionally left blank.

1.0 Introduction

This product automates Intel® Trusted Execution Technology (Intel® TXT), Trusted Platform Modules (TPM 1.2) and asset tag (ATAG) provisioning. 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 and ATAG provisioning. Intel® PTE 2.0 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 2.0 solves:

- Automates the TXT/TPM Activation in BIOS console.
- ATAG Provisioning in TPM 1.2.

What Intel® PTE 2.0 does not solve:

- TPM 1.2 hardware provisioning.
- Discovery of TXT/TPM supported hardware in given DC.
- TXT Provisioning/Launch in Linux distribution.

1.3 Requirements

Following are the requirements for Intel® PTE 2.0:

- BMC IP configured Target Intel® TXT Node, which should be in DC powered off state.
- Ubuntu 12.04 VM to install Intel® PTE 2.0 binary file.
- OEM SYSCFG tools.
- Intel® Cloud Integrity Technology (if ATAG provisioning is required).
- 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 2.0.

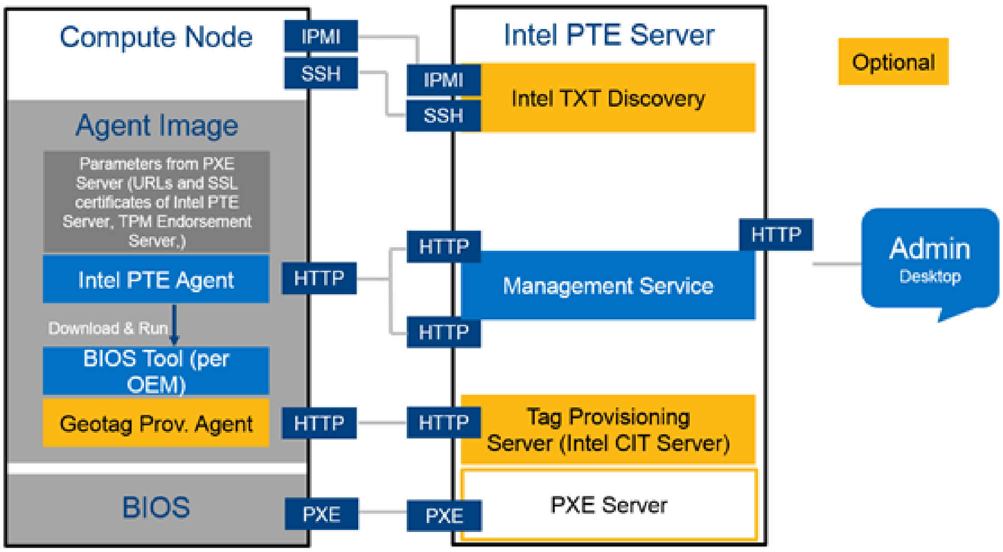


Figure 1. High-Level Solution Architecture (Version 2.0)

1.5 Deployment Topology

Figure 2 shows the deployment topology.

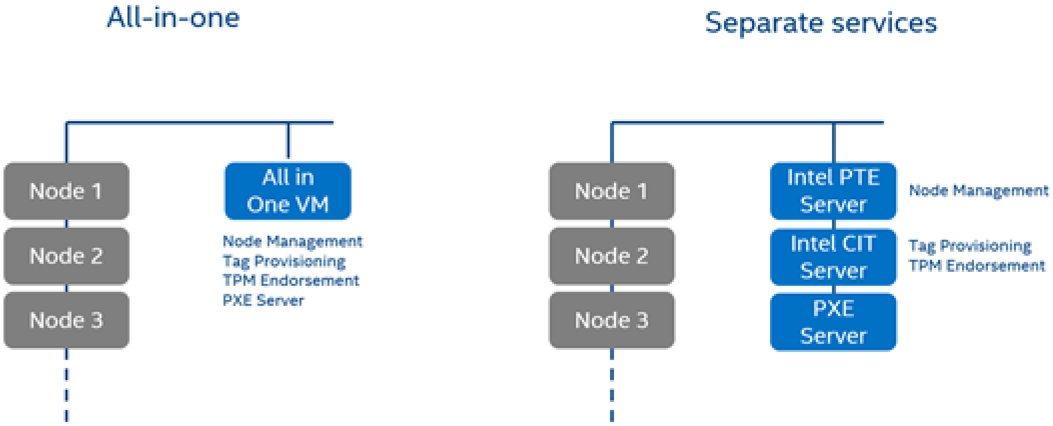


Figure 2. Deployment Architecture

Notes:

- The deployment topology is validated in a IPXE environment.
- Intel® Cloud Integrity Technology is required only when ATAG provisioning is requested.
- Intel® Platform Trust Enabler Appliance is shipped as a binary file and validated in Ubuntu 12.04.

1.6 Server Execution Flow

Figure 3 shows the high-level execution flow.

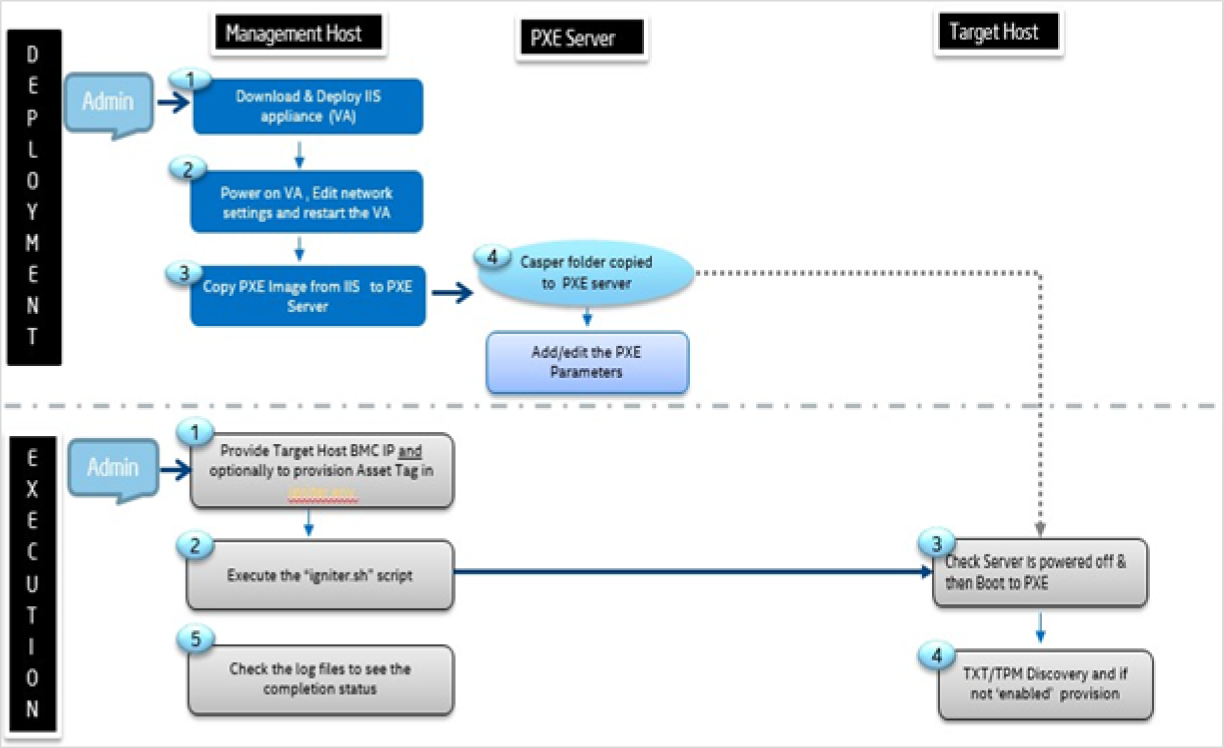

Management Host
PXE Server
Target Host
DEPLOYMENT
Admin
1 Download & Deploy IIS appliance (VA)
2 Power on VA , Edit network settings and restart the VA
3 Copy PXE Image from IIS to PXE Server
4 Casper folder copied to PXE server
Add/edit the PXE Parameters
EXECUTION
Admin
1 Provide Target Host BMC IP and optionally to provision Asset Tag in
2 Execute the "igniter.sh" script
3 Check Server is powered off & then Boot to PXE
4 TXT/TPM Discovery and if not 'enabled' provision
5 Check the log files to see the completion status

Figure 3. Deployment and Execution High-Level Flow

2.0 Installation

To install Intel® PTE 2.0, execute the following steps:

1. Download and install *pte-2.0-SNAPSHOT.bin* in plain vanilla Ubuntu 12.04 VM.

```
$ pte password <admin password> --permissions *:*
#  default credentials = admin/password
$ ./pte-2.0-SNAPSHOT.bin
```

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. Connect to the PTE2 Portal.
5. Add the BMC address of the Target Node.
6. 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 2.0 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.
3. Ensure the Intel® Cloud Integrity Technology is up and running, and copy the *ssl.crt.pem* to the PXE NFS share (path = */opt/mtwilson/configuration/ssl.crt.pem*).

Note: Copy the *cacheoff_withdefault.xml* file to the PXE NFS share to use default XML for asset tag provisioning.

Following are the **ATAG variables** that need to be added as PXE variable/parameter:

```
atag_server='https://<CIT IP>:8443/mtwilson/v2'
atag_cert='http://<PXEserverIP>/nfsshare/ssl.crt.pem'
atag_accept=yes
atag_username=<admin>
atag_password=<password>
atag_xml='http://<PXESERVER>/nfsshare/cacheoff_withdefault.xml'
PTE_SERVER=http://<PTESERVER_priv_ipaddress>/v1\
BIOS_PASSWORD='<password>'
```

2.1.1 Reference Screen Shots for PXE Configuration

Sample *menu.ipxe* file:

```
:iistestkn
echo "####################################"
echo "#   KAMAL PXEBOOT HAS STARTED...   #"
echo "####################################"
sleep 2
echo Booting ISO image of KAMAL using PXE server 10.1.68.101
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}:${nfs-root2}/kamal/casper/vmlinuz
echo Loading initrd...
sleep 3
initrd nfs://${nfs-server}:${nfs-root2}/kamal/casper/initrd.gz
sleep 3
echo "Loading variables for Asset Tag and Ignition server..."
imgargs vmlinuz root=/dev/nfs boot=casper netboot=nfs nfsroot=${nfs-server}:${nfs-root}/kamal
locale=en_US.UTF-8 atag_username=tagadmin atag_accept=yes atag_password=password
atag_cert='http://192.168.19.20/nfsshare/ssl.crt.pem'
atag_server='https://192.168.19.108:8443/mtwilson/v2'
atag_xml='http://192.168.19.20/nfsshare/cacheoff_withdefault.xml'
PTE_SERVER=http://192.168.19.117/v1 BIOS_PASSWORD='P@ssw0rd'
sleep 5
boot || goto failed
goto start
```

Sample *boot.ipxe.cfg* file:

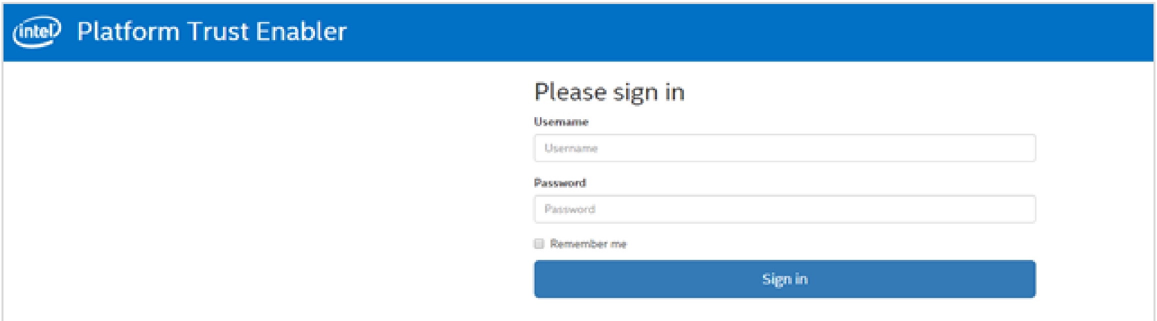
```
#!ipxe
# NFS server used for menu files and other things
# must be specified as IP, as some distros don't do proper name resolution set nfs-server
192.168.19.20
set nfs-root /home/exports set nfs-root2 /home/exports2
# Base URL used to resolve most other resources
# Should always end with a slash
#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

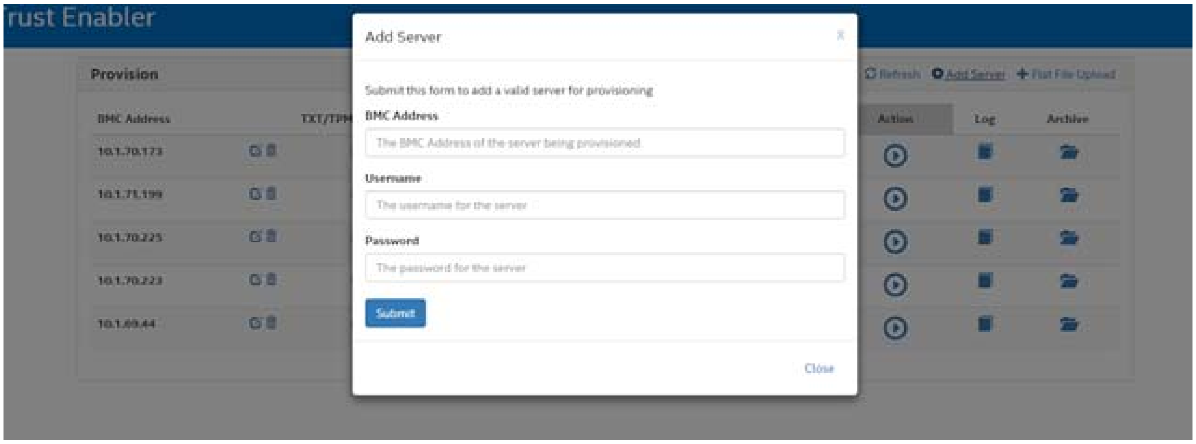
1. Connect the portal using https service.

   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.)



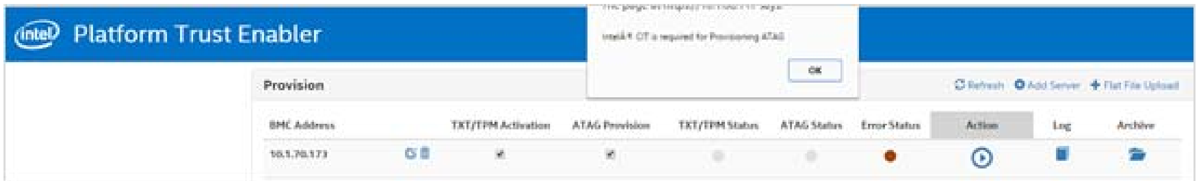
3. Select **Portal > Login> Add Server** and enter the BMC Address.



Submit this form to add a valid server for provisioning

BMC Address	TXT/TPM	Action	Log	Archive
10.1.70.173		⏵		
10.1.71.199		⏵		
10.1.70.225		⏵		
10.1.70.223		⏵		
10.1.69.44		⏵		

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

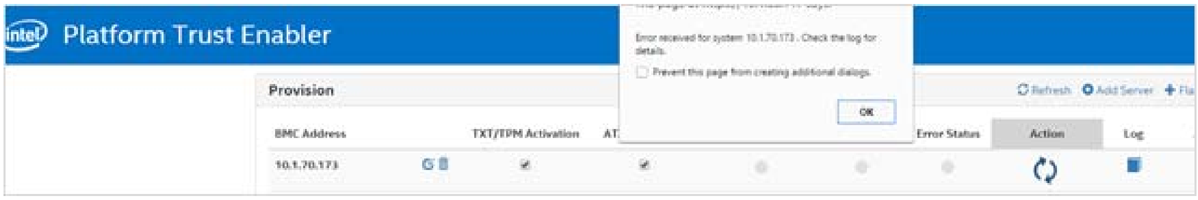


Intel® CIT is required for Provisioning ATAG

BMC Address	TXT/TPM Activation	ATAG Provision	TXT/TPM Status	ATAG Status	Error Status	Action	Log	Archive
10.1.70.173	✓	✓	●	●	●	⏵		

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

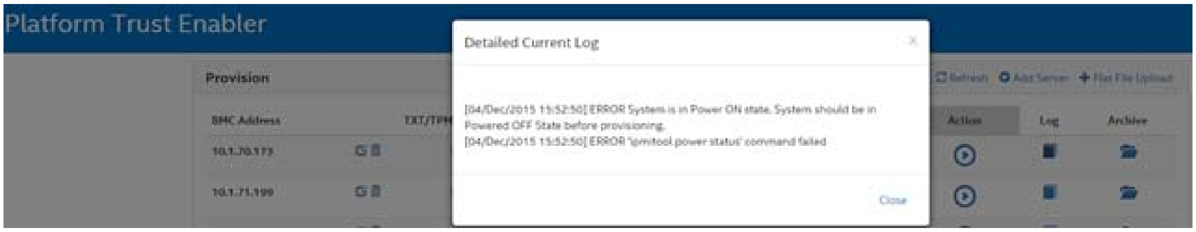
Note: The Intel® Cloud Integrity Technology instance should be up and running to provision the ATAG, and ATAG variables should be defined as PXE variables.



Error received for system 10.1.70.173 . Check the log for details.

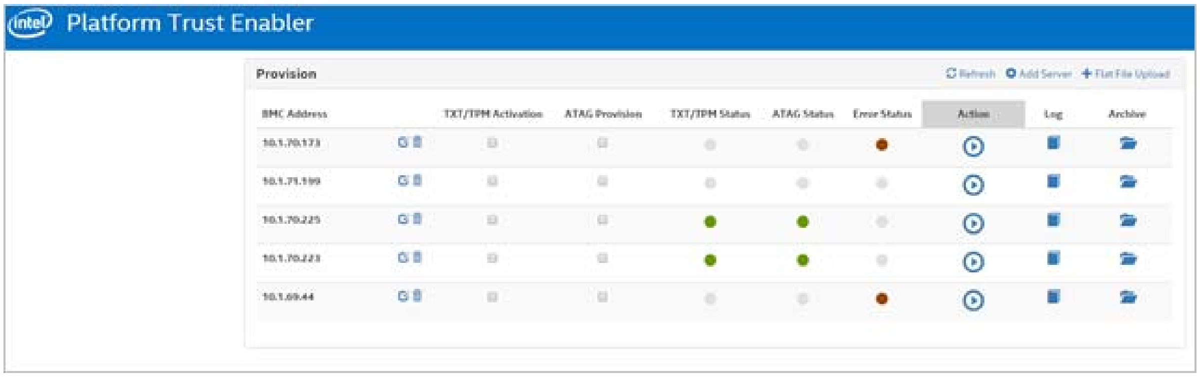
□ Prevent this page from creating additional dialogs.

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

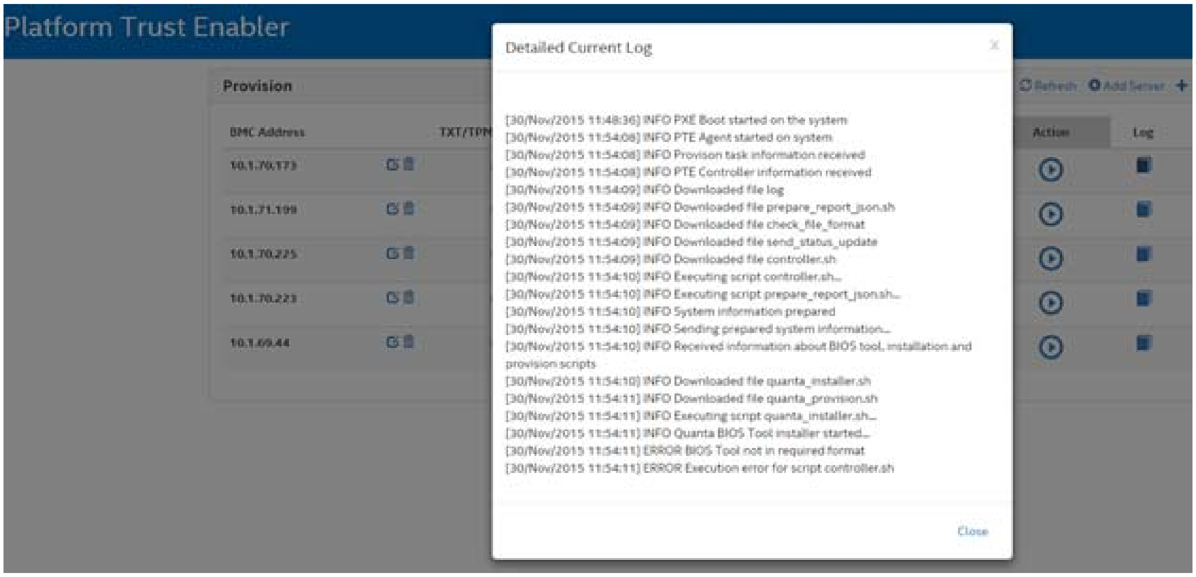


```
[04/Dec/2015 15:52:50] ERROR System is in Power ON state. System should be in Powered OFF State before provisioning.
[04/Dec/2015 15:52:50] ERROR 'ipmitool power status' command failed
```

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.

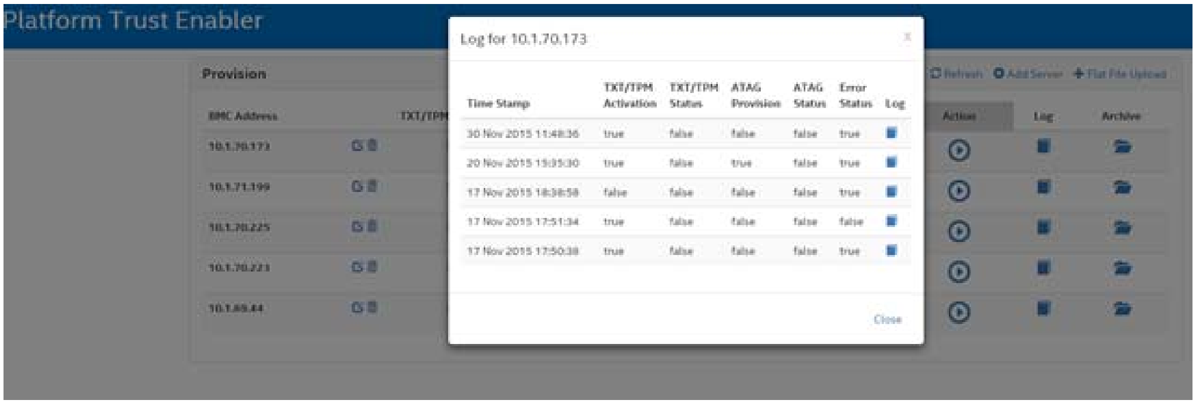


BMC Address		TXT/TPM Activation	ATAG Provision	TXT/TPM Status	ATAG Status	Error Status	Action	Log	Archive
10.1.70.173		□	□	○	○	●	▶		
10.1.71.199		□	□	○	○	○	▶		
10.1.70.225		□	□	🟢	🟢	○	▶		
10.1.70.223		□	□	🟢	🟢	○	▶		
10.1.69.44		□	□	○	○	●	▶		



Detailed Current Log

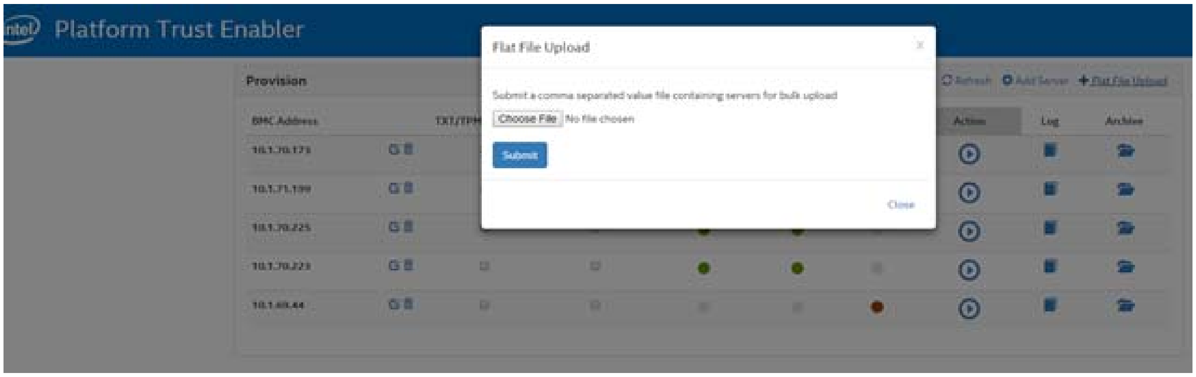
```
[30/Nov/2015 11:48:36] INFO PXE Boot started on the system
[30/Nov/2015 11:54:08] INFO PTE Agent started on system
[30/Nov/2015 11:54:08] INFO Provison task information received
[30/Nov/2015 11:54:08] INFO PTE Controller information received
[30/Nov/2015 11:54:09] INFO Downloaded file log
[30/Nov/2015 11:54:09] INFO Downloaded file prepare_report_json.sh
[30/Nov/2015 11:54:09] INFO Downloaded file check_file_format
[30/Nov/2015 11:54:09] INFO Downloaded file send_status_update
[30/Nov/2015 11:54:09] INFO Downloaded file controller.sh
[30/Nov/2015 11:54:10] INFO Executing script controller.sh...
[30/Nov/2015 11:54:10] INFO Executing script prepare_report_json.sh...
[30/Nov/2015 11:54:10] INFO System information prepared
[30/Nov/2015 11:54:10] INFO Sending prepared system information...
[30/Nov/2015 11:54:10] INFO Received information about BIOS tool, installation and
provision scripts
[30/Nov/2015 11:54:10] INFO Downloaded file quanta_installer.sh
[30/Nov/2015 11:54:11] INFO Downloaded file quanta_provision.sh
[30/Nov/2015 11:54:11] INFO Executing script quanta_installer.sh...
[30/Nov/2015 11:54:11] INFO Quanta BIOS Tool installer started...
[30/Nov/2015 11:54:11] ERROR BIOS Tool not in required format
[30/Nov/2015 11:54:11] ERROR Execution error for script controller.sh
```



Log for 10.1.70.173

Time Stamp	TXT/TPM Activation	TXT/TPM Status	ATAG Provision	ATAG Status	Error Status	Log
30 Nov 2015 11:48:36	true	false	false	false	true	🟦
20 Nov 2015 15:35:30	true	false	true	false	true	🟦
17 Nov 2015 18:38:58	false	false	false	false	true	🟦
17 Nov 2015 17:51:34	true	false	false	false	false	🟦
17 Nov 2015 17:50:38	true	false	false	false	true	🟦

7. Feature: Flat file Upload.

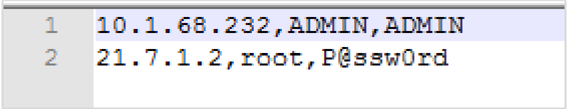


Flat File Upload

Submit a comma separated value file containing servers for bulk upload

Choose File No file chosen

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



```
10.1.68.232,ADMIN,ADMIN
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	R720	2.1.3	Dtk v4.3 [syscfg Version 4.4.0000jar00]
Intel EPSD	S2600GZ	R02.04.0003	System Configuration Utility Version 12.0 Build 10
SuperMicro	X9DRD-iF/LF	R3.0b	Supermicro Update Manager (for UEFI BIOS) V1.2.1 (2014.04.21)(x86_64)
Quanta	S210-X12RS V2	S2RS4A13	AMISCE Utility Version 2.01.1030
HP	BL460C G8	I31 08/02/2014	HP Toolkit V12.0

5.0 Tested Scenarios

Out of the Box Configuration:

- TPM/Intel® TXT provisioning only.
- ATAG provisioning only.
- TPM/Intel® TXT/ATAG provisioning.

CIT Managed TA Host:

- TPM/Intel® TXT provisioning if it is purposely disabled.
- ATAG provisioning only.
- TPM/Intel® TXT/ATAG provisioning provided TPM is owned by Intel® CIT.

CIT Managed Non-TA Host:

- TPM/Intel® TXT provisioning if it is disabled purposely.
- ATAG provisioning only.
- TPM/Intel® TXT/ATAG provisioning.

TPM	TXT	TXT/TPM Activation Requirement	ATAG Provisioning Requirement
Off	Off	Yes	No
On	On	Yes	No
Off	Off	Yes	Yes
On	On	Yes	Yes
On	Off	Yes	Yes
On	Off	Yes	No
Load Default		Yes	Yes
Load Default		Yes	No

6.0 Appendix

6.1 Workaround to Provision ATAG in DELL/HP Server

Case 1: Out-of-Box Server:

1. Initiate TXT/TPM Activation through PTE.
2. Initiate ATAG provisioning through PTE separately.

Case 2: ESXi Installed Machine:

1. Manually clear TPM.
2. Manually activate TXT/TPM or initiate through PTE, but do not let it boot to ESXI after successful activation.
3. Manually boot to ATAG PXE image (see the *Intel® Cloud Integrity Technology 3.0 Product Guide* for more information).
4. Initiate TXT/TPM activation through PTE.

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/

LEGAL

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.