



# **Intel® Trusted Device Setup (Intel® TDS) Program Notifications and Tools Release Supporting Intel® Management Engine (Intel® ME) 14/15/16**

**Corporate Release Notes - NDA**

---

***Revision 1.2***

***February 2021***

***Intel vPro® Series Release***

**Intel Confidential**



You may not use or facilitate the use of this document in connection with any infringement or other legal analysis. You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

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

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

All product plans and roadmaps are subject to change without notice.

The products described 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.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [intel.com](https://www.intel.com).

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.

© Intel Corporation. Intel, vPro, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries.

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

Copyright © 2020-2021, Intel Corporation. All rights reserved.

# Contents

1	Introduction .....	5
1.1	Scope of Document .....	5
1.2	Acronyms.....	5
2	Release Kit Summary .....	6
2.1	Release Kit Details.....	6
2.2	Kit Overview .....	6
2.3	Intel® TDS Kit Contents.....	6
2.3.1	Intel® TDS Tools .....	6
3	General Information .....	8
3.1	Supporting Documentation for Intel® TDS .....	8
3.2	Known Issues for Intel® TDS.....	8
3.3	Hardware Configurations .....	8
3.4	Supported OS .....	8
3.5	Intended Audience .....	9
4	Important Notes .....	10
4.1	General.....	10
4.2	Intel® Sealing Tool .....	10
5	Kit Details.....	11
6	Issue Status Definitions .....	12
7	Known Issues.....	13
8	Closed Issues .....	14
9	Archived Closed Issues .....	15





## Revision History

Document Number	Revision Number	Description	Revision Date
633393	1.0	• Initial release	November 2020
	1.1	• Update Sealing Tools Versions to 1.0.5.0	November 17, 2020
	1.2	• Update Sealing Tools Versions to 1.0.6.0	February, 2021

§ §

# 1 Introduction

---

## 1.1 Scope of Document

This document provides:

- Program Level Known Issues
- Intel® TDS Tools component level details of the downloaded kit and the contents of each folder in the kit.

## 1.2 Acronyms

Term	Description
Intel® PMT	Intel® Platform Measurement Tool
Intel® PTT	Intel® Platform Trust Technology
Intel® RST	Intel® Rapid Storage Technology
Intel® ST	Intel® Sealing Tool
Intel® SVT	Intel® Seal Validation Tool
Intel® TDS	Intel® Trusted Device Setup
ISV	Independent Software Vendor
OS	Operating System
PMF	Platform Measurement File
SED	Self-Encrypted Drive

## 2 Release Kit Summary

This document covers Intel® Trusted Device Setup Tools for the below corporate platforms.

### 2.1 Release Kit Details

<b>Kit Release</b>	<ul style="list-style-type: none"> <li>Intel® Tools SW with Intel® TDS support</li> </ul>
<b>Target Platform(s)</b>	<ul style="list-style-type: none"> <li>Comet Lake Corporate SKUs Platform</li> <li>Rocket Lake Corporate SKUs Platform</li> <li>Tiger Lake Corporate SKUs Platform</li> <li>Alder Lake Corporate SKUs Platform</li> </ul>

### 2.2 Kit Overview

The kit can be downloaded from the following Intel® VIP location (<https://platformsw.intel.com/>).

**Note:** A username and password are required to access the website and to log in. User must have an account created to access.

- After logging in, click the link **View All Kits** on the left side of the web page.
- Click the corresponding kit number to be downloaded.
- Select** and **Open** the appropriate kit component.
- The Supporting Documentation folder under the selected component contains the following supporting documentation:
  - Release Notes** – This document gives an overview of the contents of the entire downloaded component. Also, provides the details on the closed and open Sightings and bugs with this kit release.
- Click the **Installation Files** folder under the selected component and extract the **.zip** kit into a folder (Example: C:\).

### 2.3 Intel® TDS Kit Contents

#### 2.3.1 Intel® TDS Tools

Components	Description
Intel® PMT	<ul style="list-style-type: none"> <li>The PMT tool is designed to capture the measurements of the sample system. The tool will be run after loading up the flash and disk image and after the shipping OS image has booted once to set the PCR registers.</li> <li>OS support: Windows* 10 and Windows* PE</li> </ul>

Components	Description
Intel® Sealing Tool	<ul style="list-style-type: none"><li>• Intel® Trusted Device Setup (TDS) Sealing allows seal the platform with the required Platform Measurements values so that enterprise can:<ul style="list-style-type: none"><li>— Verify that the platform has not been tampered after leaving manufacturing</li><li>— Verify that the platform is configured exactly as expected during manufacturing</li></ul></li><li>• OS support: Windows* 10 and Windows* PE</li></ul>
Intel® Seal Validation Tool	<ul style="list-style-type: none"><li>• Intel® Trusted Device Setup Seal Validation Tool allows the end user to perform a local attestation of Intel TDS system components for functional validation purposes.</li><li>• OS support: Windows* 10</li></ul>

§ §

## 3 General Information

---

### 3.1 Supporting Documentation for Intel® TDS

Customers are recommended to download the latest revision of the following documents from [intel.com](https://intel.com).

Document Title	Document Number
Intel® Trusted Device Setup Manufacturing Flow	#615437
Intel® Trusted Device Setup Customer Communication	#615402
Intel® Trusted Device Setup Compliance Guide	#612203

### 3.2 Known Issues for Intel® TDS

- There is a known issue when enabling both Intel® Trusted Device Setup (Intel® TDS) and Windows\* Defender System Guard in manufacturing:
  - During the boot of the Intel® TDS sealed system, if the system enters hibernation (S4) prior to Intel® TDS attestation, the hibernate resume fails and results in a reboot.
- For systems that may experience early re-boots in BIOS (pre-End of DXE boot phase):
  - If this occurs while the device is sealed, Intel® TDS boot counters will indicate that Intel® TDS did not execute on all boots causing the Intel® TDS health attestation service to interpret, which is an indication of tampering.
  - If these early reboots are considered, a valid BIOS flow and not an indication of tampering, then the OEM should disable the Intel® TDS boot counter check in the health attestation service to prevent failure of Intel® TDS health check.

### 3.3 Hardware Configurations

This release supports the following HW configurations:

- CML
- RKL
- TGL
- ADL

### 3.4 Supported OS

- This release supports Windows\* 10.



## **3.5 Intended Audience**

OEM and ODM integration, testing and validation.

**§ §**

## 4 Important Notes

---

### 4.1 General

- **Sealing Tool 1.0.6.0**

- Updated OpenSSL to version 1.1.1i
- Fixed minor security issues

- **Seal Validation Tool 1.0.6.0**

- Removed support for the Disk Measurements BOM file location volume mismatch bypassing
- Changed Disk Measurements validation to verify only partitions that are present on the boot device
- Updated OpenSSL to version 1.1.1i
- Fixed minor security issues

### 4.2 Intel® Sealing Tool

- Intel® recommends customers to use the latest iRST Driver 17.8 Production Release available for download in Kit (1024401)

§ §

## 5 Kit Details

---

The table below lists the components of this Intel® TDS release

Component Name	Version Number
Intel® PMT	2.19.1.1
Intel® Sealing tool	01.0.6.0
Intel® SVT	01.0.6.0

§ §

## 6 *Issue Status Definitions*

---

This document provides sightings and bugs report for Intel® TDS.

**Known Issues:** This category will display all Known Issues since the Alpha release, and will remain in this section until fixed or noted otherwise. "Known Issues" are still under investigation and may or may not be root cause.

**Closed Issues:** This category will only display closed issues within the current kit release. After each release, old issues will be dropped down to the "Archive" section and then new closed issues will take its place back up top for the next release. If an issue is posted in this section, it will indicate that the issue has been verified and fixed within the kit that is being released.

**Archive - Fixes in Previous Kits:** This category will display all closed issues that were closed in their respected kit#. This section will serve as a history of fixed issues.

§ §

## 7 Known Issues

Issue #	Description	Details
NA	NA	NA

§ §



**Closed Issues**

## 8 *Closed Issues*

Issue #	Description	Details
NA	NA	NA

§ §

## 9 Archived Closed Issues

Issue #	Description	Details
22010955838	[lenovo_drift_2][WW26'20][TDS] Cannot perform sealing on SSD with 2TB storage	<p><b>Affected Component:</b> Platform Measurement Tool</p> <p><b>Root Cause:</b> The error is due to the PMT is getting the TPM log file with -DRTM behind that generated by the TXT, which only contains PCR 17-22. The latest v2.17 has fixed the LBA 0x7fffffff.issues as well.</p> <p><b>Symptoms:</b> The log shows the LBA range 7fffffff-7fffffff in the metadata do not match it in phy HDD</p> <p><b>Affected OS:</b> N/A</p> <p><b>Workaround:</b> N/A</p>
2209931324	[lenovo_knockout][WW50'19][TDS] SVT Validate: Seal log events validation fail: Incorrect Boot counter value.	<p><b>Affected Component:</b> Sealing Tool and Seal Validation Tools</p> <p><b>Root Cause:</b> Message reported as "Error" when it should be a "Warning"</p> <p><b>Symptoms:</b> Tool behavior issued an ERROR when "Incorrect Boot counter value" condition occur.</p> <p><b>Affected OS:</b> N/A</p> <p><b>Workaround:</b> N/A</p>

§ §