Dell Trusted Device User Guide

Dell Trusted Device

Contents

Notes, Cautions, And Warnings

NOTE: A **NOTE** indicates important information that helps you make better use of your product

CAUTION: A **CAUTION** indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A **WARNING** indicates a potential for property damage, personal injury, or death.

Technical Advisories

The Dell Trusted Device agent is part of the Dell SafeBIOS product portfolio. The Trusted Device agent includes the following:

- BIOS Verification
- BIOS Events & Indicators of Attack
- Image Capture
- Intel ME Verification
- Security Risk Protection Score
- Dell Event Repository and SIEM integration

BIOS Verification provides customers with affirmation that devices are secured below the operating system, a place where IT administrator visibility is lacking. It enables customers to verify BIOS integrity using an off-host process without interrupting the boot process. After the Trusted Device agent runs on the endpoint, a pass or fail result (0 or 1) displays in some of these locations:

- Web browser
- Command line
- Registry entry
- Event Viewer
- Logs

BIOS Events & Indicators of Attack enables administrators to analyze events in the Windows Event Viewer that may indicate bad actors targeting BIOS on enterprise endpoints. Bad actors change BIOS attributes to gain access to enterprise computers locally or remotely. These attack vectors can be monitored then mitigated through the BIOS Events & Indicators of Attack features' ability to monitor BIOS attributes.
The Intel Management Engine (Intel ME) is an independent microcontroller that is built into Intel processor chipsets manufactured starting in 2008. Intel ME provides an interface between the operating system, hardware, and BIOS. Additionally, Intel ME is granted extensive system-level privilege and runs in every power state. The Trusted Device agent scans and verifies that Intel ME firmware is present and untampered.
Security Risk Protection Score enables administrators to determine the security risk level of computers in their enterprise.
Trusted Device scans for security solutions and assigns a score per overall risk assessment.
Trusted Device includes the Dell Event Repository and can be integrated with SIEM solutions with support for following features:

- BIOS Verification
- BIOS Events & Indicators of Attack
- Image Capture
- Security Risk Protection Score

Contact Dell ProSupport for Software

Call 877-459-7304, extension 4310039 for 24×7 phone support for your Dell product.
Also, online support for Dell products is available at **dell.com/support**. Online support includes drivers, manuals,

technical advisories, FAQs, and emerging issues.
Be sure to help support quickly connect you to the right technical expert by having your Service Tag or Express Service Code available when you call.
For phone numbers outside of the United States, see **Dell ProSupport for Software international phone numbers**.

New Features and Functionality v5.10

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
  - Precision DT 3660
  - XPS NB 9720
- Dell Trusted Device (DTD) cloud services have been updated to return a standardized JSON result to client to simplify verification.
- The feature Indicators of Attack has been updated to utilize the BIOS attribute back end services for improved speed and more robust data access.

Resolved Security Advisories v5.10

No security advisories exist.

Resolved Technical Advisories v5.10

No technical advisories exists.

Technical Advisories v5.10

- The event queue signing key is validated so that the key is not easily available in the application memory. [DPS-1341]

New Features and Functionality v5.9

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
  - Latitude 7440
  - Precision 5680
  - Precision 5480
  - Latitude 3340

Resolved Security Advisories v5.9

No security advisories exist.

Resolved Technical Advisories v5.9

- In rare cases, the DTD client was writing excessive log messages to the Service.log file. This scenario is

resolved in this release. [DPS-8038]
- The JSON Payload and Signature Data for BV/MEV/SCV has been updated to enable a consistent procedure for basic result validation and parsing. [DPS-7681]

Technical Advisories v5.9

- In some scenarios, the DTD client may log excessive Path Integrity entries to the Windows Event Log on service start. Hence, the DTD client has temporarily disabled the Path Integrity based Windows Event Log entries. [DPS-7690]

New Features and Functionality v5.8

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
  - XPS 9305
  - Optiplex DT 7410 All-in-one
  - Latitude 7430
  - Latitude 7530
  - Precision 3570

Resolved Security Advisories v5.8

- No security advisories exist.

Resolved Technical Advisories v5.8

- The Dell Trusted Device service.log contained some NULL characters, which could affect the results of some string searches in the service.log. These NULL characters have been removed. [DPS-7505]
- In rare cases, Dell Trusted Device Intel Management Engine verification could erroneously return a failure. This has been resolved. [DPS-4216]

Technical Advisories v5.8

- No technical advisories exist.

New Features and Functionality v5.7

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
  - Precision 3470
  - Precision 5570
  - Precision 7670
  - Precision 7770
- The system type 32-bit operating system is no longer supported.

- New APIs are created for Security Score web services to add JSON web token authentication.
- Dell Command | Update support is added to check for new application updates and upgrade the application to its latest version.
- Enhanced the Microsoft Intune integration to add the SCV results to the **results.json** file and to the registry when BIOS verification complete a verification request.

Resolved Security Advisories v5.7

- No security advisories exist.

Resolved Technical Advisories v5.7

No technical advisories exist.

Technical Advisories v5.7

- No technical advisories exist.

New Features and Functionality v5.6

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
  - Latitude 3140
  - Latitude 5540
  - Precision 3260 Compact
  - Precision 3450 Small Form Factor
  - Precision 3480
  - OptiPlex XE4
  - OptiPlex 7010
  - XPS 13 Plus 9320

Resolved Security Advisories v5.6

- No security advisories exist.

Resolved Technical Advisories v5.6

- The Secured Component Verification (On Cloud) now includes improved error management for measurement collection. [DPS-6718]
- The Device registration workflow for Security Score is enhanced. [DPS-7111]
- The Secured Component Verification now supports ECC-P384 certificates. [DPS-7248]

Technical Advisories v5.6

- No technical advisories exist.

New Features and Functionality v5.5

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
  - OptiPlex 3000
  - OptiPlex 5000
  - XPS 9530
  - XPS 9730
- Intel ME Verification and Secured Component Verification (On Cloud) responses are now cryptographically signed allowing for external verification of the results.

Resolved Security Advisories v5.5

- Trusted Device certificate verification workflows have been hardened. [DPS-5587]
- BIOS Verification signature validation has been hardened. [DPS-5588]

Resolved Technical Advisories v5.5

- An issue resulting in missing Image Capture entries in Event Viewer is resolved. [DPS-6760]
- The Secured Component Verification (On Cloud) registration workflow is improved. [DPS-7167]

Technical Advisories v5.5

- The Trusted Device Event Repository Client Registry Generator does not currently generate the correct registry values. As a workaround, manually create the client registry values. For more information, see Configure the Trusted Device agent in the **Dell Trusted Device Event Repository Configuration Guide**. [DPS-7110]

New Features and Functionality v5.4

- **BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:**
  - OptiPlex 3090
  - OptiPlex 5090
  - OptiPlex 7090
  - Precision 3650 Tower

Resolved Security Advisories v5.4

- The Intel ME Verification logging validation workflow is hardened. [DPS-6631]

Resolved Technical Advisories v5.4

- Device registration workflows are enhanced for BIOS Verification and Intel ME Verification in Trusted Device

v5.4. [DPS-4266]

- BIOS Verification now uses improved methods to query the BIOS measurement database. [DPS-6551]
- An issue resulting in BIOS Verification errors in the service log is resolved. [DPS-6719]

Technical Advisories v5.4

- No technical advisories exist.

New Features and Functionality v5.3

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
  - Latitude 3120
  - Latitude 5430 Rugged
  - Latitude 7330
  - Precision 3450
- Trusted Device now writes the following message to Event Viewer when an outdated BIOS version is detected: Your BIOS version be out of date, see **dell.com/support**. For information about updating your BIOS, see KB article **129365**

Resolved Security Advisories v5.3

- This product release contains security updates as disclosed in the Dell Security Advisory DSA-2023-074. For more information, **see Dell Security Advisories and Notices website**.
- BIOS Events and Indicator of Attack detection for the Precision 3650 is improved. [DPS-3753]
- The BIOS Verification image validation workflow is hardened. [DPS-6298]

Resolved Technical Advisories v5.3

- An issue resulting in a driver error when installing Trusted Device on the Optiplex 7090 is resolved. [DPS-6264]
- An issue resulting in incomplete Image Captures after a BIOS Verification failure is resolved. [DPS-6412]

Technical Advisories v5.3

- No technical advisories exist.

New Features and Functionality v5.2

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now supports the following platform:
  - Latitude 9330

Resolved Security Advisories v5.2

- The BIOS Verification image measurement mechanism has been hardened. [DPS-6067]

Resolved Technical Advisories v5.2

- No technical advisories exist.

Technical Advisories v5.2

- BIOS Verification now writes the following warning to Windows Event Viewer when a BIOS version is out of date: Your BIOS version may be out of date, see **dell.com/support**. [DPS-6417]

New Features and Functionality v5.1

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
  - XPS 9315
  - XPS 9315 2-in-1
- Intel ME Verification now supports the Latitude 9430.

Resolved Security Advisories v5.1

- No security advisories exist.

Resolved Technical Advisories v5.1

- BIOS Verification failures now produce Image Captures as expected. [DPS-5675]

Technical Advisories v5.1

- No technical advisories exist.

New Features and Functionality v5.0

- Trusted Device now includes Secured Component Verification. Secured Component Verification is a supply-chain assurance offering that enables you to verify the integrity of the components inside your Dell computer. Trusted Device compares component details on your computer against a certificate containing the unique system component IDs generated and signed by Dell during factory-assembly process. Secured Component Verification verifies the following components:
  - Processor (CPU)
  - Trusted Platform Module (TPM)
  - Fixed Storage
  - Onboard Networking
  - Memory (RAM)
  - Motherboard

    - System Information

      Trusted Device performs component verification after initial installation and every startup. For each component, Trusted

      Device writes a timestamped pass or fail to the Windows Event Viewer. For more information, see the **Trusted Device Installation and Administrator Guide**.
- BIOS Events & Indicators of Attack now supports the following platforms:
    - Latitude 5421
    - Latitude 7320 Detachable
    - Latitude 7420
    - Latitude 9520

Resolved Security Advisories v5.0

- No security advisories exist.

Resolved Technical Advisories v5.0

- No technical advisories exist.

Technical Advisories v5.0

- No technical advisories exist.

New Features and Functionality v4.11

- No technical advisories exist.

Resolved Security Advisories v4.11

- No security advisories exist.

Resolved Technical Advisories v4.11

- No technical advisories exist.

Technical Advisories v4.11

- No technical advisories exist.

New Features and Functionality v4.10

- BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME Verification now support the following platforms:
    - Precision 5470

- XPS 9520

Resolved Security Advisories v4.10

- No security advisories exist.

Resolved Technical Advisories v4.10

- An issue resulting in proxy errors in the Service log is resolved. [DPS-5526]

Technical Advisories v4.10

- No technical advisories exist.

New Features and Functionality v4.9

- Trusted Device v4.9 includes a new version of the Trusted Device Event Repository. See **https://hub.docker.com/r/dellemc/dtd-event-repository** for more information.

Resolved Security Advisories v4.9

- The Trusted Device driver authentication workflow has been hardened. [DPS-5589]

Resolved Technical Advisories v4.9

- An issue resulting in non-Impersonate errors in the service log is resolved. [DPS-5801]

Technical Advisories v4.9

- No technical advisories exist.

New Features and Functionality v4.8

- The Latitude 9420 is now supported by BIOS Events & Indicators of Attack.
- The Trusted Device Event Repository now supports PBKDF2 password storage. You can manually configure the PBKDF2 element or build it using the appsettings generator utility. For more information, see the **Trusted Device Installation and Administrator Guide**.

Resolved Security Advisories v4.8

- No security advisories exist.

Resolved Technical Advisories v4.8

- An issue resulting in malformed BIOS Event data is resolved. [DPS-5800]

Technical Advisories v4.8

- When configuring the required appsettings.json, the Signing Certificate value must match or be derived from the Jwt Certificate value. For more information, see Configure the appsettings.json file in the **Trusted Device Installation and Administrator Guide**. [DPS-5764]

New Features and Functionality v4.7

- The Trusted Device agent now detects unsupported BIOS versions. After detection, Trusted Device writes the following error in the Registry, Service log, and Windows Event Viewer:
  BIOS Verification: 14 (BIOS Version Not Currently Supported)
  For more information, see the **Trusted Device Installation and Administrator Guide**.
- The following platforms are now supported by BIOS Verification, BIOS Events & Indicators of Attack, and Intel ME
  Verification:
  - OptiPlex 5400 All-in-One
  - OptiPlex 7000
  - OptiPlex 7400 All-in-One
- The following platforms are now supported by BIOS Events & Indicators of Attack:
  - Latitude 7320 2-in-1
  - Precision 5560

Resolved Security Advisories v4.7

- No security advisories exist.

Resolved Technical Advisories v4.7

- No technical advisories exist.

Technical Advisories v4.7

- In rare scenarios, Trusted Device v4.7 may write “Unable to impersonate user for setting proxy” errors to the Service log, which indicates a failed BIOS Verification attempt. As a workaround, reboot the computer. [DPS-5526]
- If BIOS Verification fails, Trusted Device does not currently perform an Image Capture on the Latitude 7420. [DPS-5675]

New Features and Functionality v4.6

- Trusted Device v4.6 now supports 64 MB SPI flash parts.

Resolved Security Advisories v4.6

- Trusted Device agent's registration workflow with the Trusted Device Event Repository has been hardened. [DPS-4643]

Resolved Technical Advisories v4.6

- No technical advisories exist.

Technical Advisories v4.6

- No technical advisories exist.

New Features and Functionality v4.5

- No technical advisories exist.

Resolved Security Advisories v4.5

- No security advisories exist.

Resolved Technical Advisories v4.5

- No technical advisories exist.

Technical Advisories v4.5

- No technical advisories exist.

New Features and Functionality v4.4

- BIOS Verification now retrieves the BIOS version that is installed during the verification process.
- Trusted Device now writes the current BIOS version and the recommended BIOS version to Windows Event Viewer.
- The Trusted Device Event Repository now supports BIOS version reporting.
- The JSON configuration files used to create custom compliance policies in Microsoft Endpoint Manager have been merged into a single file.

Resolved Security Advisories v4.4

- The Trusted Device driver has been hardened. [DPS-4473, DPS-4469]

Resolved Technical Advisories v4.4

- An issue resulting in a false error in the Service logs is resolved. [DPS-4464]

Technical Advisories v4.4

- In rare situations, the recommended BIOS version that is written in Windows Event Viewer identifies non-production BIOS versions as recommended. Verify the latest BIOS version for your computer at **dell.com/support**. [DPS-4529]

New Features and Functionality v4.3

- No technical advisories exist.

Resolved Security Advisories v4.3

- Trusted Device leaf certificate validation is improved. [DPS-4106]
- The Trusted Device driver validation workflow has been hardened. [DPS-4374]

Resolved Technical Advisories v4.3

- No technical advisories exist.

Technical Advisories v4.3

- Trusted Device does not currently validate non-production BIOS version from Dell. Non-production BIOS versions include engineering builds, debug builds, and validation releases provided by Dell ProSupport for troubleshooting. [DPS-4561]
- The ADDLOCAL and REMOVE parameter functions have been removed from the Trusted Device installer. To add or remove Trusted Device features, uninstall and reinstall Trusted Device with the wanted features.

  NOTE: If the ADDLOCAL or REMOVE parameters are used during installation, the installer fails. [DPS-4660]

New Features and Functionality v4.2

- No technical advisories exist.

Resolved Security Advisories v4.2

- The Trusted Device agent verification workflow for Access Control Lists and Symbolic Links has been hardened. [DPS 2498]
- The Trusted Device driver validation workflow has been hardened. [DPS-4374]

Resolved Technical Advisories v4.2

- No technical advisories exist.

Technical Advisories v4.2

- To see Trusted Device compliance and results in Microsoft Endpoint Manager, it is currently required to create

a unique custom script package for each policy that is created with DTDComplianceRules-BiosVerification.json and DTDComplianceRules-Installation.json. See the **Trusted Device Installation and Administrator Guide** for more information. [DPS-4472]

- BIOS Verification currently validates only BIOS versions 1.8.1 and newer on the Latitude 5591. [DPS-4477]

New Features and Functionality v4.1

- Microsoft Endpoint Manager is a highly versatile platform containing a combination of services that IT administrators use.
  Microsoft Endpoint Manager includes the following services:
  - Azure Active Directory
  - Co-management
  - Configuration Manager
  - Desktop Analytics
  - Endpoint Manager admin center
  - Intune
  - Windows Autopilot

These services and tools are used to manage and monitor mobile devices, desktop computer, virtual machines, embedded devices, and servers. See **this Microsoft article** for more information about Microsoft Endpoint Manager. Administrators can create compliance policies in the Endpoint Manager admin center to ensure that Trusted Device is protecting computers below the operating system.
Trusted Device uses PowerShell scripts and agent-level configuration to communicate endpoint compliance and sends results to Microsoft Endpoint Manager. See the **Trusted Device Installation and Administrator Guide** for more information.

- Trusted Device v4.1 includes a new version of the Trusted Device Event Repository. See **https://hub.docker.com/r/dellemc/dtd-event-repository** for more information.
- The Trusted Device Event Repository now supports configurable API path prefixes. See the **Trusted Device Installation and Administrator Guide** for more information.

Resolved Security Advisories v4.1

- No security advisories exist.

Resolved Technical Advisories v4.1

- No technical advisories exist.

Technical Advisories v4.1

- The -noncefile and -noncestring parameters are not currently supported. [DPS-4322]

New Features and Functionality v4.0

- The following platforms are now supported by BIOS Verification:

    - Latitude 5421
    - Latitude 5521
    - Precision 3560
    - Precision 3561
    - Precision 5560
    - Precision 5760
    - Precision 7560
    - XPS 9310
    - XPS 9310 2-In-1
- The following platforms are now supported by Intel ME Verification:
    - Latitude 5320
    - Latitude 5420
    - Latitude 5421
    - Latitude 5520
    - Latitude 5521
    - Latitude 7320
    - Latitude 7320 2-In-1
    - Latitude 7420
    - Latitude 7520
    - Latitude 9520
    - Precision 3560
    - Precision 3561
    - Precision 5560
    - Precision 5760
    - Precision 7560
    - Precision 7760
    - XPS 9310
    - XPS 9310 2-In-1

Resolved Security Advisories v4.0

- No security advisories exist.

Resolved Technical Advisories v4.0

- A rare issue resulting in computer crash after applying Windows updates to a computer protected by Trusted Device is resolved. [DPS-4142]
- An issue resulting in mishandled validation of SAN leaf certificates when Trusted Device is installed on a non-English operating system is resolved. [DPS-4197]
- An issue resulting in BIOS Events & Indicator of Attack incorrectly writing duplicate Information events to Event Viewer is resolved. [DPS-4232]

Technical Advisories v4.0

- No technical advisories exist.

New Features and Functionality v3.9

- Trusted Device v3.9 includes a new version of the Trusted Device Event Repository. See **https://hub.docker.com/r/dellemc/dtd-event-repository** for more information.
- The Trusted Device Event Repository now includes a utility that creates the required appsettings.json file for SIEM communication. For more information, see the **Trusted Device Installation and Administrator Guide**.
- The Trusted Device Event Repository now includes a utility that creates the client registry entries that are required to deliver results to the Event Repository. For more information, see the **Trusted Device Installation and Administrator Guide**.
- Administrators can now retrieve browser-based results for the Trusted Device Events Repository version running. To see the version of the Event Repository running in your environment, type the following into a browser: https://<EventRepositoryhostnameorIPaddress>:/siem/api/v1/version

  NOTE: The Event Repository container must be running for results to display.

Resolved Security Advisories v3.9

- No security advisories exist.

Resolved Technical Advisories v3.9

- No technical advisories exist.

Technical Advisories v3.9

- No technical advisories exist.

New Features and Functionality v3.8

- The following platforms are now supported by BIOS Verification:
  - Latitude 9420
  - Latitude 9520

Resolved Security Advisories v3.8

- Trusted Device permission handling in the Windows Registry is improved. [DPS-3823]

Resolved Technical Advisories v3.8

- An issue resulting in false BIOS Verification failure after restarting a computer is resolved. [DPS-2555]

Technical Advisories v3.8

- Trusted Device does not currently support installations for non-English versions of Windows. As a workaround, install Windows using English configuration and then change your language settings. To change Windows language, see **this Microsoft article**. [DPS-4141, DPS-4197, DDPSUS-3047]

New Features and Functionality v3.7

- Trusted Device v3.7 now supports Windows 11.

Resolved Security Advisories v3.7

- The workflow for building the Trusted Device Event Repository container is hardened. [DPS-3706]

Resolved Technical Advisories v3.7

- Upgrades no longer result in multiple errors in the service logs. [DPS-3645]
- Errant Event Log data no longer displays in Security Risk Protection Score data. [DPS-3765]

Technical Advisories v3.7

- No technical advisories exist.

New Features and Functionality v3.6

Trusted Device v3.6 now includes Intel ME Verification. The Intel Management Engine (Intel ME) is an independent microcontroller that is built into Intel processor chipsets manufactured starting in 2008. Intel ME provides an interface between the operating system, hardware, and BIOS. Additionally, Intel ME is granted extensive system-level privilege and runs in every power state.
The Trusted Device agent scans and verifies that Intel ME firmware is present and untampered after initial installation, startup, and every 24 hours. For additional information including types of events and event location, see **the Trusted Device Installation and Administrator Guide**.

- Trusted Device v3.6 now included SIEM integration. Security Information Event Management (SIEM) solutions aggregate data from multiple sources in your enterprise. SIEM enables administrators to identify trends and unusual behavior or to perform real-time analysis of alerts that are generated by applications and hardware. Data aggregated through SIEM can be transformed into charts and graphs on a dashboard to facilitate use. This helps administrators ensure that the enterprise maintains security compliance and protection against bad actors.

  Trusted Device can be integrated with SIEM solutions and supports the following features:
  - BIOS Verification
  - BIOS Events & Indicators of Attack
  - Image Capture
  - Security Risk Protection Score

The Trusted Device Event Repository must be installed to deliver Trusted Device results to a SIEM solution. For more information, see the **Trusted Device Installation and Administrator Guide**.

Resolved Security Advisories v3.6

- BIOS Verification certificate handling has been hardened. [DPS-3139]

Resolved Technical Advisories v3.6

- No technical advisories exist.

Technical Advisories v3.6

- Errant Event Log data may display in Security Risk Protection Score data. This data should be ignored. [DPS-3765]

New Features and Functionality v3.5

- No technical advisories exist.

Resolved Security Advisories v3.5

- Signing Certificates have been updated in the Trusted Device back-end, Versions prior to v3.5 will not properly retrieve BIOS Verification data after September 2021. For more information, see KB article **190190**. [DPS-3749]

Resolved Technical Advisories v3.5

- BIOS Verification browser-based results now display as expected when BIOS Verification is run interactively. [DPS-3267, DPS-3670]

Technical Advisories v3.5

- No technical advisories exist.

Documents / Resources

	**Dell Trusted Device** [pdf] User Guide Trusted Device, Trusted, Device

References

- **User Manual**