Dell Trusted Device

Technical Advisories v2.1

DELL EMC

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.

Rev. A01

Contents

1

Technical Advisories

The Dell Trusted Device agent is part of the Dell SafeBIOS product portfolio. The Trusted Device agent includes BIOS Verification, Image Capture, and BIOS Events & Indicators of Attack.

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.

Contact Dell ProSupport

For questions or concerns with BIOS Verification, please visit our chat support here.

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell product.

Additionally, 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 us 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 International Phone Numbers.

New Features and Functionality v2.1

- Trusted Device documentation (previously BIOS Verification) is now located on the following landing page: https://www.dell.com/support/home/us/en/19/product-support/product/trusted-device/docs.
- The BIOS Verification agent is now rebranded to the Dell Trusted Device agent.

  NOTE: BIOS Verification remains a feature of the Dell Trusted Device agent.
- Trusted Device now runs as a Windows service.
- 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 & Indicator of Attack features' ability to monitor BIOS attributes. If the Trusted Device agent is active on the computer, BIOS Events & Indicators of Attack runs every 12 hours by default.

  It is recommended using a SIEM product to retrieve logs and events. Administrators should provide results to their SOC team to determine appropriate remediation strategies.

  Find BIOS Events & Indicator of Attack notifications in Event Viewer under **Windows Logs > System** with Source type **Trusted Device**.
- To change BIOS attributes interval polling, set the following registries.
  - This entry configures the time period in seconds between BIOS attribute sweeps.

    HKLM\SOFTWARE\Dell\TrustedDevice\

    DWORD=SecondsBetweenAttributeSweeps

    Minimum value in seconds = 3600 (1 hour)

Maximum value = 172800 (48 hours)

Default = every 12 hours

Value (in decimal) = 3600 - sweeps occur every one hour

Value (in decimal) = 172800 - sweeps occur every 48 hours

- This entry changes the delay in milliseconds between each individual BIOS attribute retrieval.

  HKLM\SOFTWARE\Dell\TrustedDevice\

  DWORD=MSBetweenAttributeReads

  Minimum value in milliseconds = 500

  Maximum value in milliseconds = 2000

  Default = every 500 ms

  Value (in decimal) = 500 - reads a different BIOS attribute every 500 ms

  Value (in decimal) = 2000 - reads a different BIOS attribute every 2000 ms

- The following platforms are supported by BIOS Events & Indicators of Attack:
  - Latitude 3301
  - Latitude 3400
  - Latitude 3500
  - Latitude 5300
  - Latitude 5300 2-in-1
  - Latitude 5400
  - Latitude 5401
  - Latitude 5500
  - Latitude 5500
  - Latitude 7200 2-in-1
  - Latitude 7300
  - Latitude 7400
  - Latitude 7400 2-in-1
  - Optiplex 7070 Ultra
  - Optiplex 7071 Tower
  - Precision 3540
  - Precision 3541
  - Precision 5540
  - Precision 7540
  - Precision 7740
  - XPS 13 7390
  - XPS 13 7390 2-in-1
  - XPS 15 7590

Resolved Technical Advisories v2.1

- The Trusted Device product version is now in logging. [DPS-1194]

Technical Advisories v2.1

- Added May 4, 2020 - The Dell Latitude 3400 and Dell Latitude 3500 currently experience an issue waking from sleep mode with Trusted Device installed. This issue is currently under investigation. Dell recommends that Trusted Device is not installed on these platforms until this issue is resolved. [DPS-1608]
- In rare occurrences, the Trusted Device agent uses excessive computer resources resulting in delayed trackpad movement. As a work around, change the MSBetweenAttributeReads value in the Registry in HKLM\SOFTWARE\Dell\TrustedDevice\. [DPS-862, DPS-1071, DPS-1076]
- In rare occurrences, the Trusted Device agent fails to load properly resulting in computer crash or incorrect BIOS Verification results. [DPS-1237]
- The Dell DiagnosticInfo utility does not properly collect text versions of the Dell Event log. [DPS-1168]
- The Trusted Device agent driver does not monitor all registry entries as expected. [DPS-1177]

- The Dell Trusted Device agent is available with the improper signature. [DPS-1213]
- All Windows Registry entries are not removed after uninstalling Trusted Device. [DPS-1387]

New Features and Functionality v1.7

- No technical advisories exist.

Resolved Technical Advisories v1.7

- Results no longer take up to 30 seconds to populate. [DPS-587]
- The Dell DiagnosticInfo utility now collects all registry information for BIOS Verification. [DPS-925]

Technical Advisories v1.7

- Logs do not currently display the installed version of BIOS Verification. [DPS-1194]

New Features and Functionality v1.6

- BIOS Verification v1.6 now supports the following platforms:
  - Latitude 3180
  - Latitude 3189
  - Latitude 3190
  - Latitude 3190 2-in-1
  - Latitude 3300
  - Latitude 3380
  - Latitude 3480
  - Latitude 3490
  - Latitude 3580
  - Latitude 3590
  - Latitude 5280
  - Latitude 5285
  - Latitude 5289
  - Latitude 5290
  - Latitude 5290 2-in-1
  - Latitude 5420
  - Latitude 5424
  - Latitude 5480
  - Latitude 5490
  - Latitude 5491
  - Latitude 5495
  - Latitude 5580
  - Latitude 5590
  - Latitude 5591
  - Latitude 7280
  - Latitude 7285
  - Latitude 7290
  - Latitude 7380
  - Latitude 7389
  - Latitude 7390
  - Latitude 7390 2-in-1
  - Latitude 7424 Rugged
  - Latitude 7480
  - Latitude 7490
  - Optiplex 3050
  - Optiplex 3050 All-in-One

- Optiplex 3060
- Optiplex 3070
- Optiplex 5050
- Optiplex 5055
- Optiplex 5060
- Optiplex 5070
- Optiplex 5250 All-in-One
- Optiplex 5260 All-in-One
- Optiplex 5270 All-in-One
- Optiplex 7050
- Optiplex 7060
- Optiplex 7070
- Optiplex 7450 All-in-One
- Optiplex 7460 All-in-One
- Optiplex 7470 All-in-One
- Optiplex 7760 All-in-One
- Optiplex 7770 All-in-One
- Optiplex XE3
- Precision 3430
- Precision 3431
- Precision 3520
- Precision 3530
- Precision 3630
- Precision 5520
- Precision 5530
- Precision 5530 2-in-1
- Precision 5820 Tower
- Precision 5820 XL Tower
- Precision 7520
- Precision 7530
- Precision 7720
- Precision 7730
- Precision 7820 Tower
- Precision 7920 XL Tower
- XPS 13 9365
- XPS 13 9380
- XPS 15 9560
- XPS 15 9570
- XPS 15 9575

Resolved Technical Advisories v1.6

- No technical advisories exist.

Technical Advisories v1.6

- In rare occurrences, BIOS Verification incorrectly interprets supported devices as unsupported. For more information, see SLN319932. [DPS-860]
- Running the Dell DiagnosticInfo utility does not currently collect all registry information for BIOS Verification. [DPS-925]

New Features and Functionality v1.5

- BIOS Verification installation now includes Dell Diagnostic Info for log collection.

Resolved Technical Advisories v1.5

- An issue resulting in false verification failure for platforms with multiple valid BIOS images is resolved. [DPS-306, DPS-307, DPS-699, DPS-820, DPS-822]

Technical Advisories v1.5

- No technical advisories exist.

New Features and Functionality v1.4

- BIOS Verification now automatically captures corrupt or tampered BIOS images on boot.
- BIOS Verification v1.4 now supports the following platforms:
  - Latitude 7220 Rugged Tablet
  - Latitude 7220 Rugged Extreme Tablet

Resolved Technical Advisories v1.4

- BIOS Verification no longer requires US time/date format to properly communicate with Dell Cloud. [DPS-700]

Technical Advisories v1.4

- No technical advisories exist.

New Features and Functionality v1.3

- BIOS Verification v1.3 now supports the following platforms:
  - Optiplex 7070
  - Optiplex 7071 Tower

Resolved Technical Advisories v1.3

- When changing the Image Store directory, BIOS Verification now verifies write access to the destination directory. [DPS-452]

Technical Advisories v1.3

- Non-US date/time formats currently yield communication errors with Dell Cloud. [DPS-700]

New Features and Functionality v1.2

- BIOS Verification v1.2 now supports the following platforms:
  - Latitude 3301
  - Latitude 7400
  - Precision 3541
  - Precision 5540
  - XPS 13 7390 2-in-1
  - XPS 15 7590
- BIOS Verification now supports Image Capture. After detecting a corrupt or tampered image, BIOS Verification copies the image to the EFI partition then to %PROGRAMDATA%\Dell\BIOSVerification\ImageCapture. Administrators can invoke image capture, configure captured image storage locations, and export most recent or all images. Each captured image is signed and named BIOSImageCaptureMMDDYYYY_HHMMSS.rcv where MMDDYYYY is the date and HHMMSS is the time of image copy.

Resolved Technical Advisories v1.2

- BIOS Verification's desktop icon is rebranded to Dell BIOS Verification Console. [DPS-143]

Technical Advisories v1.2

- BIOS Verification does not currently differentiate between upgrade or new install in the graphic user interface. [DPS-448]
- When changing the Image Store directory, BIOS Verification does not currently check for write access to the destination directory. [DPS-452]
- If the PublicKeyBlob registry value does not exist prior to running the export argument, an error occurs. [DPS-464]
- In some scenarios, results can take up to 30 seconds to populate. [DPS-587]

New Features and Functionality v1.1

- The following platforms are supported with BIOS Verification v1.1:
  - Latitude 5401
  - Latitude 7540
  - Latitude 7740
  - XPS 7390
- BIOS Verification now uses Microsoft's assembly versioning convention.

Resolved Technical Advisories v1.1

- BIOS Verification results now render properly in Internet Explorer. [DPS-9]
- BIOS Verification results now open in the user's default browser. [DPS-142]
- Authentication between BIOS Verification and Dell Cloud is hardened. [DPS-241]

Technical Advisories v1.1

- No technical advisories exist.