Dell Trusted Device

Installation and Administrator Guide 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

Introduction

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 the Dell Trusted Device agent, go to chat support.

Call 877-459-7304, extension 4310039 for 24x7 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.

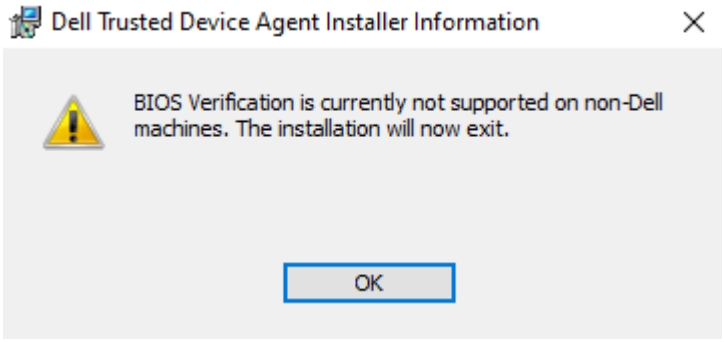
For phone numbers outside of the United States, see Dell ProSupport International Phone Numbers.

2

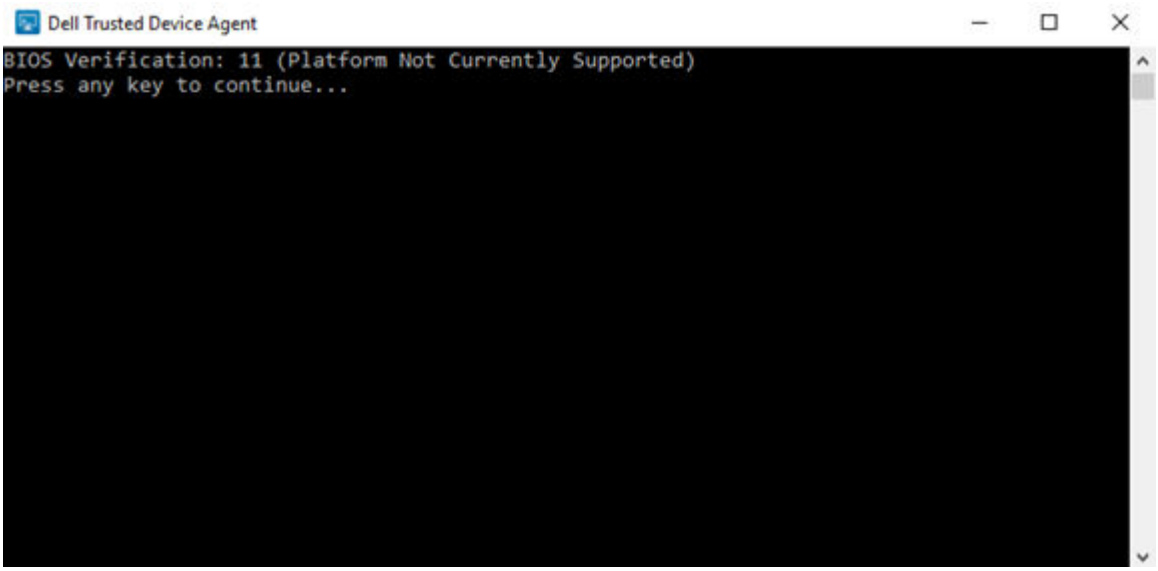
Requirements

- See the table below for a list of supported platforms.

NOTE: If the Trusted Device agent is installed on non-Dell platforms, the following error displays.



NOTE: If the Trusted Device agent is installed or run on an unsupported platform, the following error displays.



Prerequisites

Prerequisites

- Microsoft .Net Framework 4.5.2 (or later) is required for the installer. The installer *does not* install the Microsoft .Net Framework component.

  All computers that are shipped from the Dell factory are preinstalled with the full version of Microsoft .Net Framework 4.5.2 (or later). To verify the version of Microsoft .Net installed, follow these instructions on the computer targeted for installation. To install Microsoft .Net Framework 4.5.2, see these Microsoft instructions.

Platforms

- The following table details supported platforms:

NOTE: An asterisk (*) indicates the BIOS Events & Indicators of Attack feature supports the platform. BIOS Verification supports all listed platforms.

Dell Computer Models

- Latitude 3180
- Latitude 3190
- Latitude 3190 2-in-1
- Latitude 3189
- Latitude 3300
- Latitude 3301 *
- Latitude 3380
- Latitude 3400 *
- Latitude 3480
- Latitude 3490
- Latitude 3500 *
- Latitude 3580
- Latitude 3590
- Latitude 5280
- Latitude 5285
- Latitude 5289
- Latitude 5290
- Latitude 5290 2-in-1
- Latitude 5300 *
- Latitude 5300 2-in-1 *
- Latitude 5400 *
- Latitude 5401 *
- Latitude 5420
- Latitude 5424
- Latitude 5480
- Latitude 5490
- Latitude 5491
- Latitude 5495
- Latitude 5500 *
- Latitude 5501 *
- Latitude 5580
- Latitude 5590
- Latitude 5591
- Latitude 7200 2-in-1 *
- Latitude 7220 Rugged Tablet
- Latitude 7220 Rugged Extreme Tablet
- Latitude 7280
- Latitude 7285
- Latitude 7290
- Latitude 7290 2-in-1
- Latitude 7300 *
- Latitude 7380
- Latitude 7389
- Latitude 7390
- Latitude 7400 *
- Latitude 7400 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 Ultra *
- OptiPlex 7071 Tower *
- 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 3540 *
- Precision 3541 *
- Precision 3630
- Precision 5520
- Precision 5530
- Precision 5530 2-in-1
- Precision 5540 *
- Precision 5820 Tower
- Precision 5820 XL Tower
- Precision 7520
- Precision 7530
- Precision 7540 *
- Precision 7720
- Precision 7730
- Precision 7740 *
- Precision 7820 Tower
- Precision 7820 XL Tower
- XPS 13 7390 *
- XPS 13 7390 2-in-1 *
- XPS 13 9365
- XPS 13 9380
- XPS 13 9560
- XPS 15 7590 *
- XPS 15 9570
- XPS 15 9575

Ports

- Ensure the Trusted Device agent can communicate with the Dell Cloud by whitelisting port 443. See the following table for more information:

Destination	Protocol	Port
service.delltrusteddevicesecurity.com	HTTPS	443
api.delltrusteddevicesecurity.com	HTTPS	443

Operating Systems

- The following table details supported operating systems:

Windows Operating Systems (32-bit and 64-bit)
• Windows 10

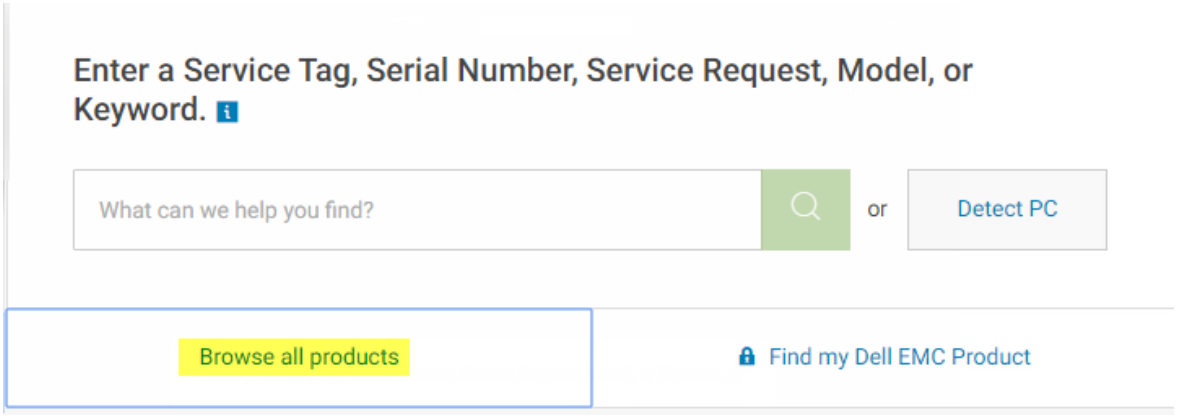
3

Download the Software

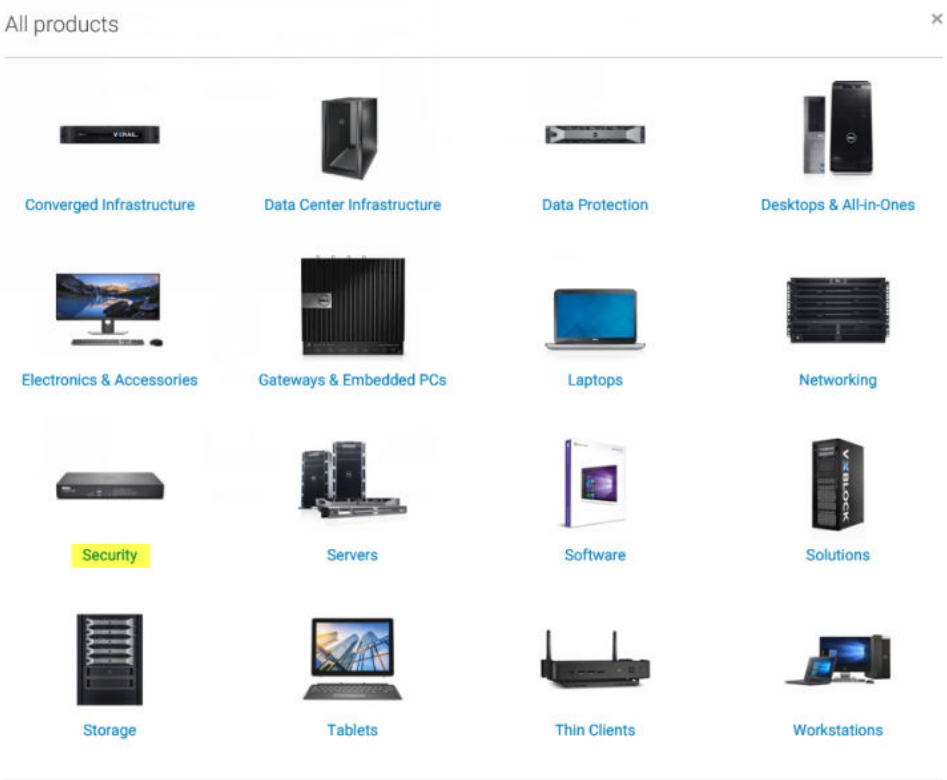
This section details obtaining the software from dell.com/support. If you already have the software, you can skip this section.

Go to dell.com/support to begin.

1. On the Dell Support webpage, select **Browse all products**.

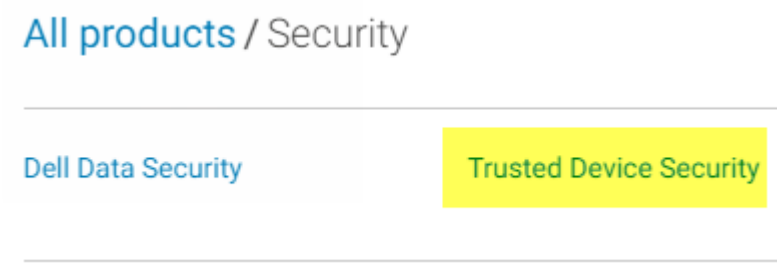


2. Select **Security** from the list of products.



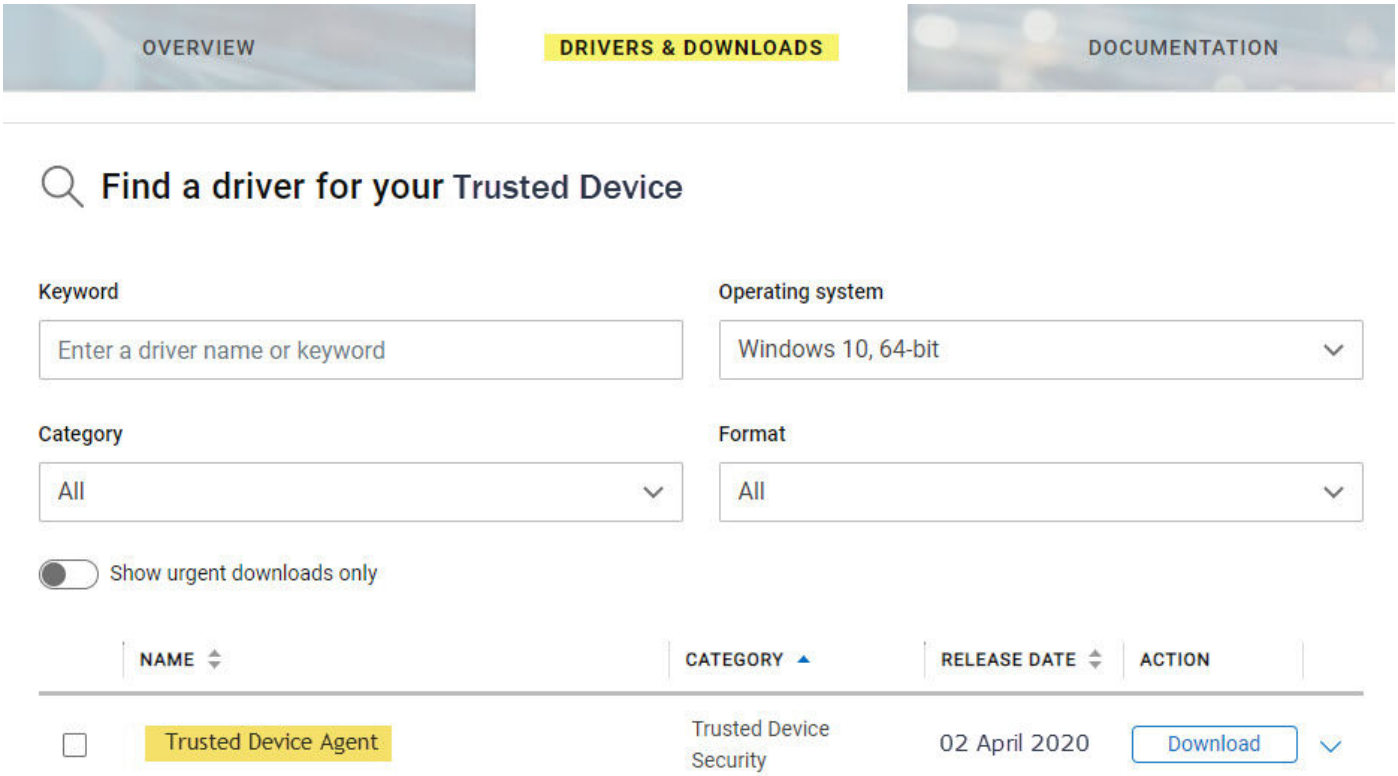
3. Select **Trusted Device Security**.

   After this selection has been made once, the website remembers.

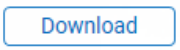


4. Select the product.

   Trusted Device
5. Select **Drivers & downloads**.
6. Select the wanted client operating system type.
7. Select **Trusted Device Agent**.



8. Select **Download** .



4

Installation

Use one of the following methods to install the Trusted Device agent:

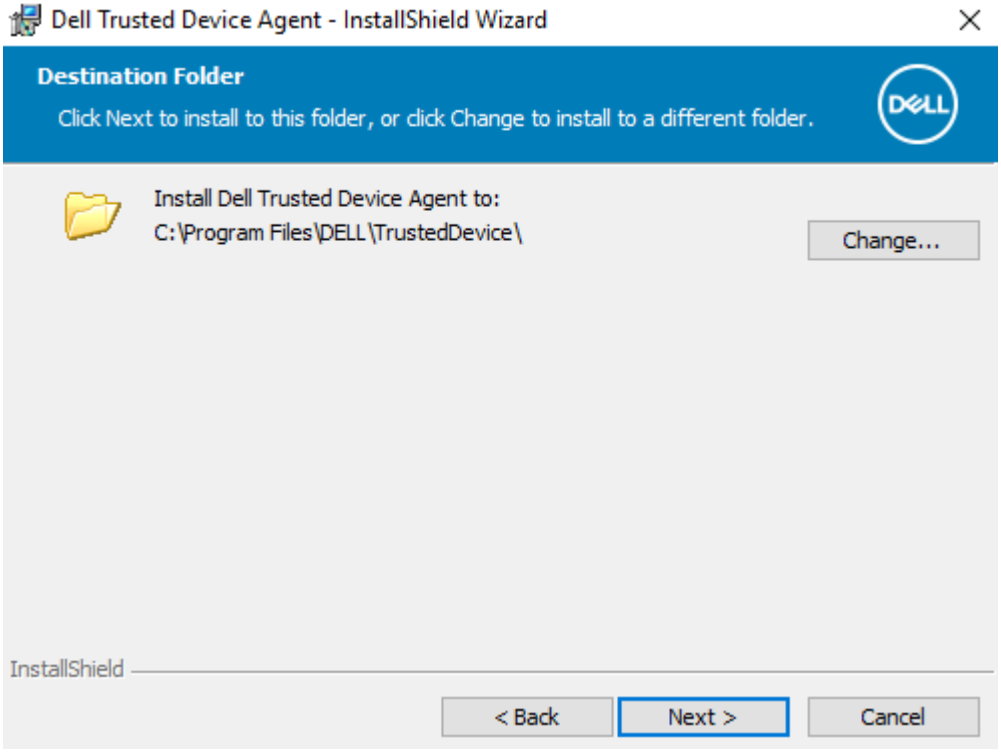
- Interactive Installation
- Command-Line Installation

Interactive Installation

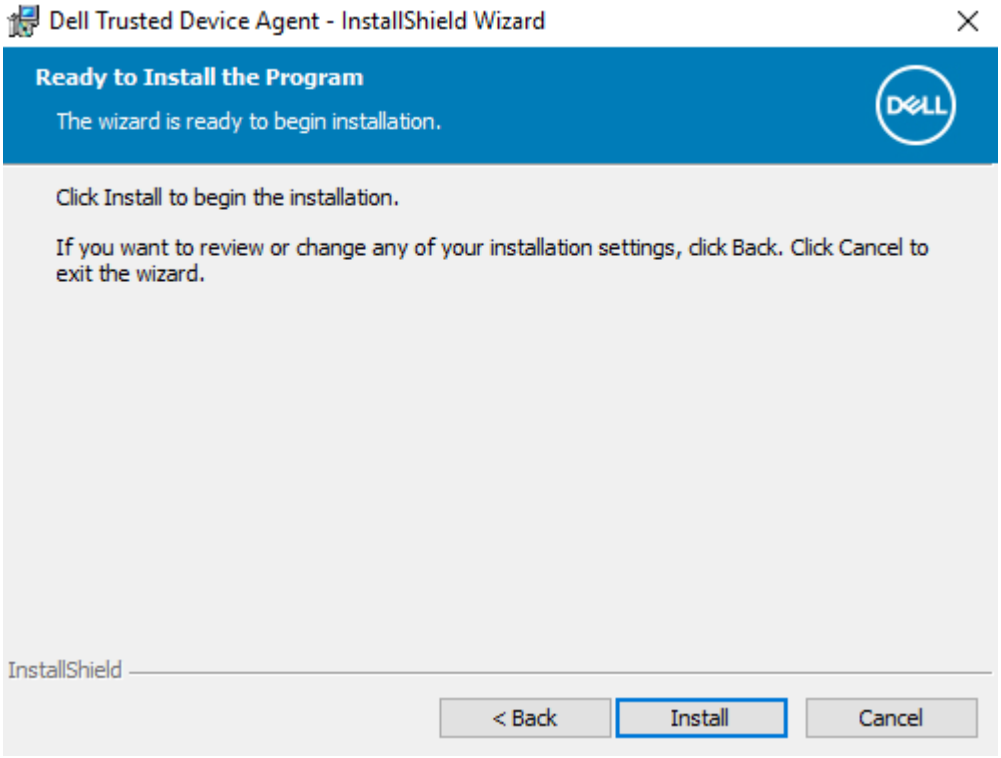
The Trusted Device agent installer requires administrative rights. The bit rate of the utility must match the architecture of the host computer operating system. Choose one of the following:

- TrustedDeviceSetup.exe - 32-bit installer
- TrustedDeviceSetup-64Bit.exe - 64-bit installer

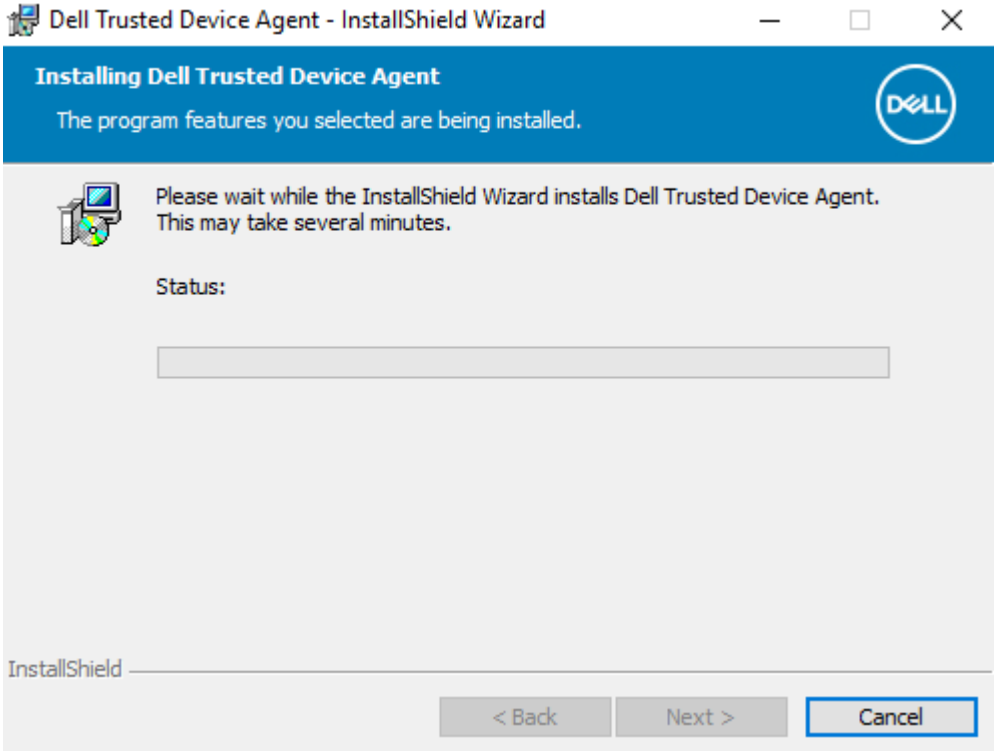
1. Copy **TrustedDeviceSetup-64Bit.exe** to the local computer.
2. Double-click **TrustedDeviceSetup-64Bit.exe** to launch the installer.
3. Click **Next** at the Welcome screen.
4. Read the license agreement, agree to the terms, and click **Next**.
5. Click **Next** to install in the default location of `C:\Program Files\Dell\TrustedDevice\`



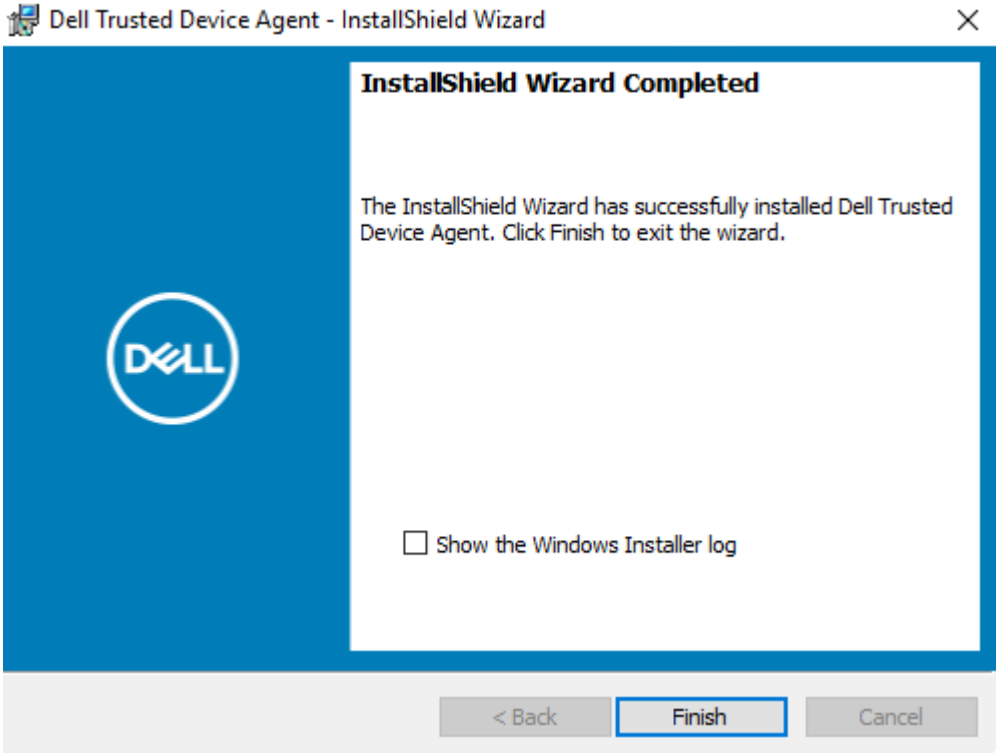
6. Click **Install** to begin the installation.



7. A status window displays but may take several minutes.



8. Click **Finish**.



After installation, a browser launches and displays results. See Results, Troubleshooting, and Remediation for more information.

Restart the computer to complete installation if prompted.

Command-Line Installation

- Be sure to enclose a value that contains one or more special characters, such as a blank space in the command line, in escaped quotation marks.
- Use these commands to install Trusted Device Agent using a scripted installation, batch files, or any other push technology available to your organization.
- Log files: Windows creates installation log files for the logged in user at %temp%, at `C:\Users\<UserName>\AppData\Local\Temp`.

  If you decide to add a separate log file when you run the installer, ensure that the log file has a unique name. Use the standard .msi command to create a log file. For example: `/l*v C:\<any directory>\<any log file name>.log`. See the example listed below.
- The installer uses basic .msi switches and display options, except where noted, for command-line installations. The switches must be specified first. The /v switch is required and takes an argument. Other parameters go inside an argument that is passed to the /v switch.

  Specify display options at the end of the argument that is passed to the /v switch to achieve the expected behavior. Do not use both /q and /qn in the same command line. Only use ! and – after /qb.

Switch	Meaning
/v	Pass variables to the .msi inside the *.exe.
/s	Silent mode

Option	Meaning
/q	No Progress dialog - restarts itself after process completion
/qb	Progress dialog with **Cancel** button, prompts for restart.
/qb-	Progress dialog with **Cancel** button - restarts itself after process completion

Option	Meaning
/qb!	Progress dialog without **Cancel** button - prompts for restart
/qb!-	Progress dialog without **Cancel** button - restarts itself after process completion
/qn	No user interface

- Parameters:

  The following table details the parameters available for the installation.

Parameters
InstallPath=path to alternate installation location

- Example Command-Line Installation

  Example Command Line to Install the Trusted Device Agent

  The bit rate of the utility must match the architecture of the operating system. Choose one of the following:

  - TrustedDeviceSetup.exe - 32-bit installer
  - TrustedDeviceSetup-64Bit.exe - 64-bit installer

- The following example installs the 32-bit Trusted Device agent with silent installation, no progress bar, installed in the default location of **`C:\Program Files\Dell\TrustedDevice\`** and installation logs in **C:\Dell**.

  ```
  TrustedDeviceSetup.exe /s /qn /l*v C:\Dell\TrustedDevice.log
  ```

- The following example installs the 64-bit Trusted Device agent with silent installation, no progress bar, installed in the default location of **C:\Program Files\Dell\TrustedDevice**.

  ```
  TrustedDeviceSetup-64Bit.exe /s /qn
  ```

Deployment and Collection

Best practice: When installing the Trusted Device agent with third-party utilities, administrators should target specific collections of devices to avoid a high volume of noise from unsupported platforms.

There are many options to target supported platforms with deployment utilities. For examples of generating collections using the Microsoft System Center Configuration Manager (SCCM) and options to target specific devices, see https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/create-collections.

Deployments are performed through SCCM based on generated collections. For more information about generating deployment tasks and scheduling across larger environments, see https://docs.microsoft.com/en-us/sccm/apps/deploy-use/deploy-applications.

Other third-party utilities use similar mechanisms. For information about PDQ Deploy options for creating collections, see https://support.pdq.com/knowledge-base/1752-viewing-and-creating-collections-in-pdq-inventory.

For additional information about deploying packages with PDQ Deploy, see https://www.pdq.com/deploy-scheduling/

5

Uninstall Trusted Device

The user uninstalling **must** be a local administrator. If uninstalling by command line, domain credentials are required.

Use one of the following methods to uninstall the utility:

- Uninstall from Apps & features
- Uninstall from the Command-Line

Uninstall from Apps & Features

1. In **Type here to search** on the taskbar, type **Apps & features**.
2. Left-click **Dell Trusted Device Agent** then left-click **Uninstall**.

Uninstall from the Command-Line

The following example uninstalls Trusted Device:

```
wmic path win32_product where (Caption like "Dell Trusted Device") call uninstall
```

6

Image Capture

Administrators can capture images of corrupted or tampered BIOS for analysis and remediation. When run, Trusted Device queries the EFI partition for a corrupt or tampered image. If an image is detected, it is copied from the EFI partition to %PROGRAMDATA%\Dell\TrustedDevice\ImageCapture. If off-host verification fails, Trusted Device copies corrupt or tampered images from memory to %PROGRAMDATA%\Dell\TrustedDevice\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 based on the following:

- If copied from the EFI partition - `BIOSImageCaptureMMDDYYYY_HHMMSS.rcv`
- If copied from memory - `BIOSImageCaptureBVSMMDDYYYY_HHMMSS.bv`

`MMDDYYYY` is the date and `HHMMSS` is the time of image copy. For Command-Line parameters, see Run the Utility.

For more information about Image Capture and the Windows Registry, see Results, Troubleshooting, and Remediation .

7

BIOS Events & Indicators of Attack

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.

To see additional information including types of events and event location, see Results, Troubleshooting, and Remediation.

8

Run the BIOS Verification Agent

Use one of the following methods to run the agent:

- Interactively
- Command Line

NOTE: If you attempt to run the BIOS Verification agent on an unsupported platform, **Platform Not Supported** displays.

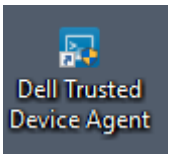
NOTE: The Dell Trusted Device agent determines Dell platform support at runtime.

Run the BIOS Verification Agent by Schedule

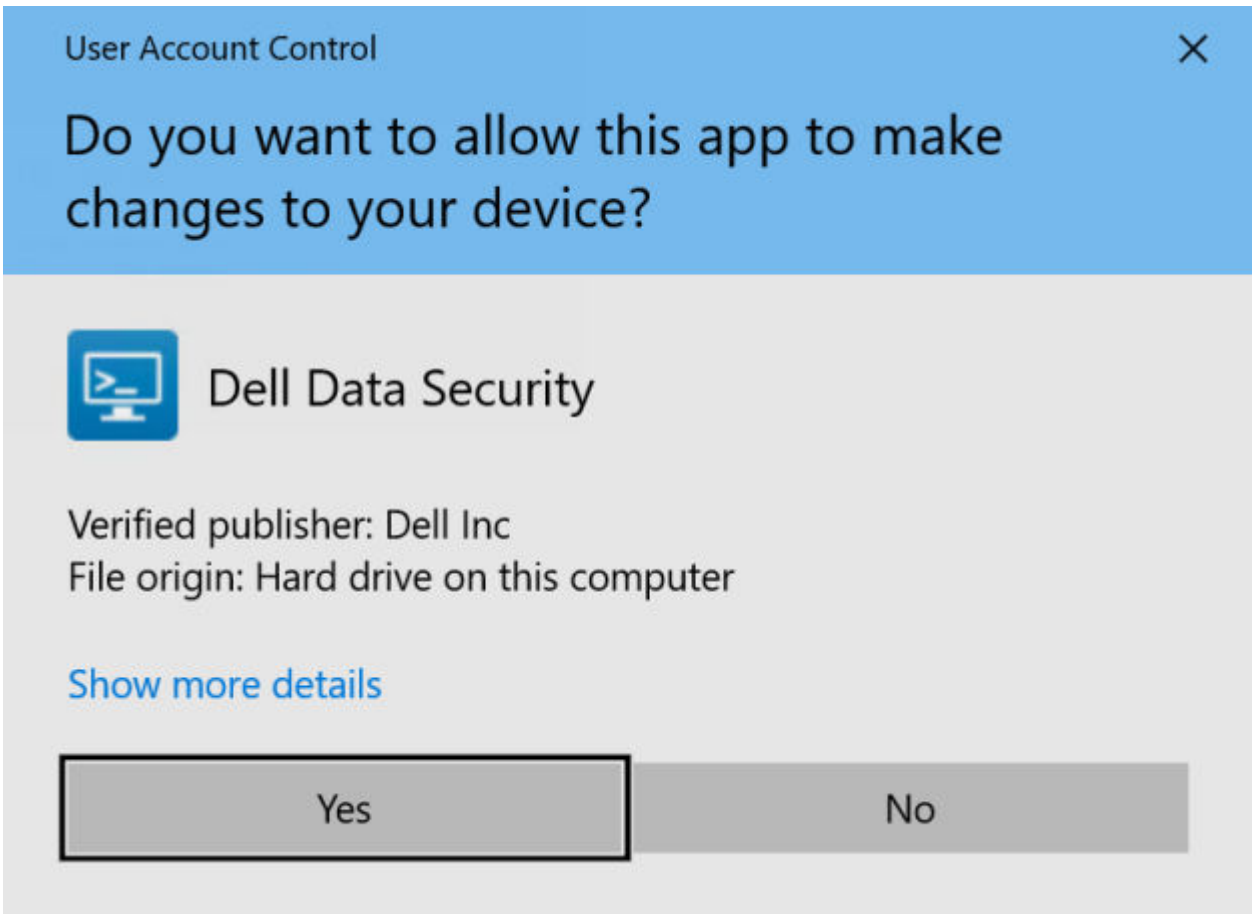
To schedule BIOS Verification agent to run at set intervals or to trigger execution by events, see Microsoft Task Scheduler documentation here.

Run the BIOS Verification Agent Interactively

1. Double-click the **Dell Trusted Device Agent** icon.



2. If User Account Control is enabled, click **Yes** to proceed.



3. A browser launches automatically and displays BIOS results.

NOTE: If the utility is unable to determine BIOS state, browser-based results do not display. See Results, Troubleshooting, and Remediation for error codes.

Run the BIOS Verification Agent with Command Line

The following table details optional command-line arguments.

Parameters	Meaning
-imagecapture	Copies the captured BIOS image to the default or specified location
-export <FolderLocation>	Exports the most recent image to a specified location
-exportall -export <FolderLocation>	Exports all images to a specified location.
-updateimagestore <FolderLocation>	Modifies the default image storage location
-headless	Suppresses browser result and display results in the Command-Line window
-noncefile <filename>	Load the file as a binary file and the contents become the nonce. If the file is larger than 1024 bytes, an ArgumentException error is thrown.

Parameters	Meaning
-noncestring <nonce>	The <nonce> parameter is a base64 encoded nonce. The string is base64 decoded, and the result becomes the nonce. If the decoded nonce is larger than 1024 bytes, an ArgumentException error is thrown.

1. Open Command Prompt with administrative privileges.
2. Go to the directory containing the utility.
3. Type **`Dell.TrustedDevice.Service.Console.exe`** then press Enter.
4. A browser launches automatically and displays BIOS results.

   NOTE: To suppress the browser result and display results in the Command-Line window, use the `-headless` flag. For example, `Dell.TrustedDevice.Service.Console.exe -headless`

   If the utility is unable to determine BIOS state, an error code displays. Error code definitions are listed in Results, Troubleshooting, and Remediation.

   NOTE: BIOS results are written to the following registry location each time the utility is run: `[HKLM\Software\Dell\BIOS Verification]` .

   NOTE: The `%ERRORLEVEL%` environment variable is updated and can be queried for results to automate silently gathering BIOS status centrally.

Commonly Used Scenarios

Running the BIOS Verification agent in repeated intervals ensures that devices remain in a protected state. Third-party utilities are commonly used to run and report back on a schedule. It is recommended targeting specific collections of devices to avoid a high volume of noise from unsupported platforms.

It is recommended that you run the BIOS Verification feature with its headless property as SYSTEM on devices to avoid interrupting users while ensuring the proper return codes.

- The following example runs the TrustedDevice agent in headless mode with logs and results written to the default location of C:\ProgramData\Dell\TrustedDevice\:

  ```
  C:\Program Files\Dell\TrustedDevice\Dell.TrustedDevice.Service.Console.exe -headless
  ```

After running the utility, query %ERRORLEVEL% to return the status of the device in question. The %ERRORLEVEL% return value can be compared against the list of error code definitions in Results, Troubleshooting, and Remediation.

Scheduling is used to automate the collection of BIOS results. Microsoft's SCCM custom task sequence can collect status reports for scheduled tasks. For more information on managing the schedule of the task sequence, see https://docs.microsoft.com/en-us/previous-versions/system-center/packs/hh967525(v=technet.10)#BKMK_Mandatory_Assignment.

To limit return results to computers supported by Trusted Device, it is recommended using a collection created with Microsoft's SCCM. For information on the options to target specific devices, see https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/create-collections.

Third-party utilities use similar retrieval mechanisms. For information on PDQ Deploy's options for creating collections, see https://support.pdq.com/knowledge-base/1752-viewing-and-creating-collections-in-pdq-inventory.

9

Results, Troubleshooting, and Remediation

This chapter details reviewing results, troubleshooting, and remediating a corrupt or tampered BIOS image.

Results

After running the BIOS Verification agent, results are written to C:\ProgramData\Dell\TrustedDevice\, the %ERRORLEVEL% environment, the Event Viewer, and the registry.

%PROGRAMDATA%

The Trusted Device agent writes logs and JSON formatted results to C:\ProgramData\Dell\TrustedDevice\.

%ERRORLEVEL% Environment

The Trusted Device agent writes pass/fail results to the %ERRORLEVEL% environment. After running the agent, administrators can query %ERRORLEVEL% to return the status of specific devices. The %ERRORLEVEL% return value can be compared against the list of error codes in the table below.

Event Viewer

The Dell Trusted Device agent writes a new notification to the Event Viewer each run and at regular intervals. Find BIOS Verification and Image Capture notifications in Event Viewer under **Application and Service Logs > Dell** with Source type BiosVerification. Find BIOS Events & Indicator of Attack notifications in Event Viewer under **Windows Logs > System** with Source type Trusted Device. Details pertaining to the events are listed in the General tab of Event Viewer. The following tables detail the BIOS Verification and BIOS Events & Indicators of Attack in Event Viewer.

BIOS Verification

Action	Level	Event ID	Task Category
Verification Passed	Warning	3	1
Verification Failed	Error	2	1
Image Captured	Warning	1	2
Duplicate Image Capture	Warning	2	2
No Image Found	Informational	3	2

BIOS Events & Indicators of Attack

Action	Level	Event ID	Task Category
Partial Indicator of Attack	Warning	1001	1
Indicator of Attack	Error	1002	1

Registry

The Trusted Device agent's results are written to the registry each time the BIOS Verification agent is run. All BIOS Verification, Image Capture, and BIOS Events & Indicators of Attack registry keys are located at HKLM\Software\Dell\TrustedDevice.

Off-host Verification

- This entry stores the pass/fail status of off-host verification in JSON format.

  HKLM\Software\Dell\BiosVerification

  Result.json

  "biosVerification":"True"=Pass

  "biosVerification":"False"=Fail

Image Capture

- This entry stores the location of the image store and is updated when the `-updateimagestore` parameter is used.

  HKLM\Software\Dell\TrustedDevice

  "ImagePathStore"=string
- Determine if an image was present on the last Image Capture run. This value will not exist if Image Capture has not run.

  HKLM\Software\Dell\TrustedDevice

  "ImagePresentOnLastRun"=DWORD

  DWORD=1 - Image was present on last run.

  DWORD=0 - Image was not present on last run.
- Image store path in which the last image was copied. This value will not exist if no images are captured.

  "LastImagePath"=string
- Timestamp of the last copied image.

  "LastCopyTimeStamp"=string
- This private key verifies the images in the store.

  "PrivateKeyBlob"=string

  Note: End users should not modify this entry as it will prevent the product from functioning properly.
- A public key used to verify the images in the store.

  "PublicKeyBlob"=string

  Note: End users should not modify this entry as it will prevent the product from functioning properly.

BIOS Attributes Polling Interval

- 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

Troubleshooting

If BIOS results are unavailable, browser-based results **do not** display. Refer to the following table for error codes.

Error Code	Meaning	Additional Information
0	Verification passed	The local BIOS is verified against a known-good Dell BIOS.
1	Verification failed	The local BIOS failed verification against a known-good Dell BIOS.
2	The verification result is tampered	The verification result is tampered. Run the Dell Trusted Device agent again. If this error persists, reinstall the Dell Trusted Device agent or contact Dell Support.
3	An unknown error occurred	The Dell Trusted Device agent's detail retrieval failed. Please run the Dell Trusted Device agent again. If this error persists, contact Dell Support.
4	An invalid command line argument was specified	A command line variable passed to the Dell Trusted Device agent is not supported. Please see the supported command line syntax for the Dell Trusted Device agent here or run the Dell Trusted Device agent with the `-help` switch or `/?`
5	The agent is running with insufficient privileges	The Dell Trusted Device agent requires local administrator rights to run.
6	An internal error has occurred	An error on the local device occurred preventing The Dell Trusted Device agent from properly running. Run Trusted Device again. If this error persists, contact Dell Support.
7	Server responded with an error or is unavailable	The Dell Trusted Device agent's server is unavailable. Validate network connectivity and that the web-based locations are accessible from the device.
8	An issue in the driver occurred	The Dell Trusted Device agent's driver failed to load. Run BIOS Verification again. If this error persists, reboot the device and try again, or contact Dell Support.
9	An error occurred because the BIOS data used to perform verification is invalid	This local BIOS is not supported with BIOS Verification. Ensure the local BIOS version is updated and run BIOS Verification again.
10	This is returned when the `-help` command line argument is specified	The Dell Trusted Device agent was run with the `-help` argument.
11	This is returned if the platform or BIOS image is not supported	The Dell Trusted Device agent does not support this device. If you believe that this device is supported, please update the BIOS version here. If this error persists, contact Dell Support.
12	An error has occurred in the Trusted Device service	Please reboot the computer and run the Dell Trusted Device agent again. If this error persists, please contact Dell Support.

Remediation

If BIOS image results fail, refer to KB article SLN300716 to update your BIOS to the latest version. Refer to KB article SLN284433 for more information about Dell BIOS.