

Dell BIOS Verification

Installation and Administrator Guide v1.7

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.

© 2019 - 2020 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Registered trademarks and trademarks used in this document: Dell™ and the Dell logo, Dell Precision™ and Latitude™ are trademarks of Dell Inc. Microsoft®, Windows®, Windows 10®, Microsoft System Center Configuration Manager®, and Task Scheduler® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners.

1 Introduction.....	4
Contact Dell ProSupport.....	4
2 Requirements.....	5
BIOS Verification Requirements.....	5
3 Architecture.....	8
4 Download the Software.....	9
5 Installation.....	11
Deployment and Collection.....	14
6 Uninstall BIOS Verification.....	15
7 Image Capture.....	16
8 Run the Utility.....	17
Run the Utility Interactively.....	17
Run the Utility with Command Line.....	18
Commonly Used Scenarios.....	19
9 Results, Troubleshooting, and Remediation.....	20
Results.....	20
Troubleshooting.....	21
Remediation.....	22

Introduction

The BIOS Verification utility provides customers with affirmation that devices are secured below the operating system, a place where IT administrator visibility is lacking. It empowers customers to verify BIOS integrity using an off-host process without interrupting the boot process. BIOS Verification is part of the Dell SafeBIOS product portfolio.

A result of passed or failed (0 or 1) is displayed in a web browser or available from command line or from the registry after BIOS Verification runs on the endpoint.

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.

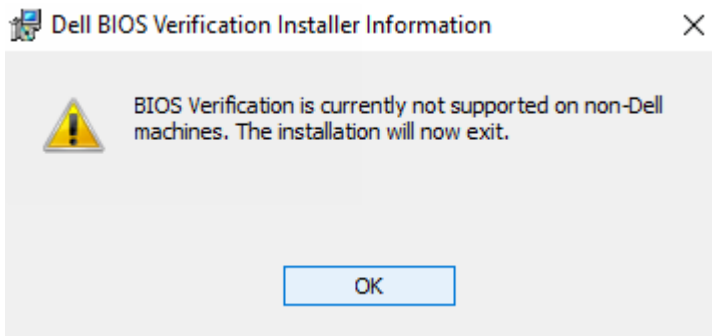
For phone numbers outside of the United States, see [Dell ProSupport International Phone Numbers](#).

Requirements

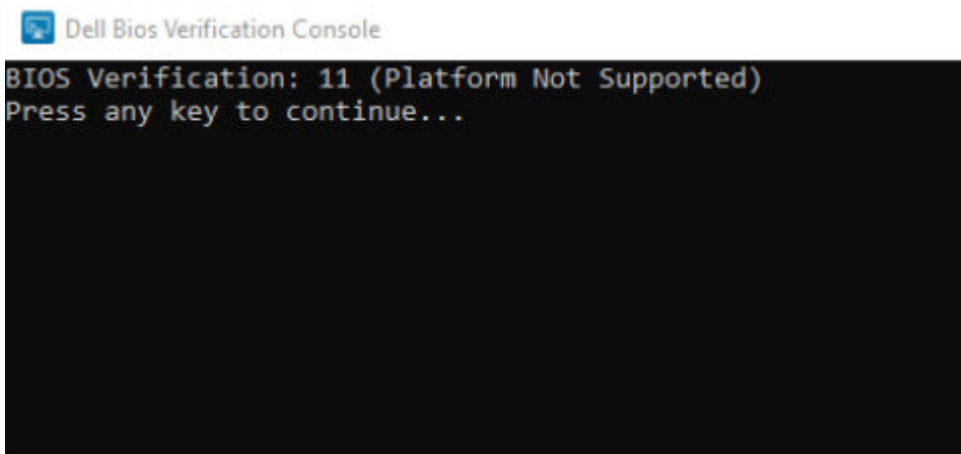
BIOS Verification Requirements

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

NOTE: The following error displays if BIOS Verification is installed on non-Dell platform.



NOTE: The following error displays if BIOS Verification is installed or run on an unsupported platform.



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 shipped from the Dell factory are pre-installed 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: [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx). To install Microsoft .Net Framework 4.5.2, see <https://www.microsoft.com/en-us/download/details.aspx?id=42643>.

Platforms

- The following table details supported platforms.

Dell Computer Models

- | | | | |
|-----------------|-----------------|------------------|---------------|
| • Latitude 3180 | • Optiplex 3050 | • Precision 3430 | • XPS 13 7390 |
|-----------------|-----------------|------------------|---------------|

Dell Computer Models

- 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 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 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 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 2-in-1
- XPS 13 9365
- XPS 13 9380
- XPS 13 9560
- XPS 15 7590
- XPS 15 9570

Ports

To ensure BIOS Verification can communicate with Dell Cloud, port 443 must be whitelisted. Refer to the following table for more information.

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

Operating Systems

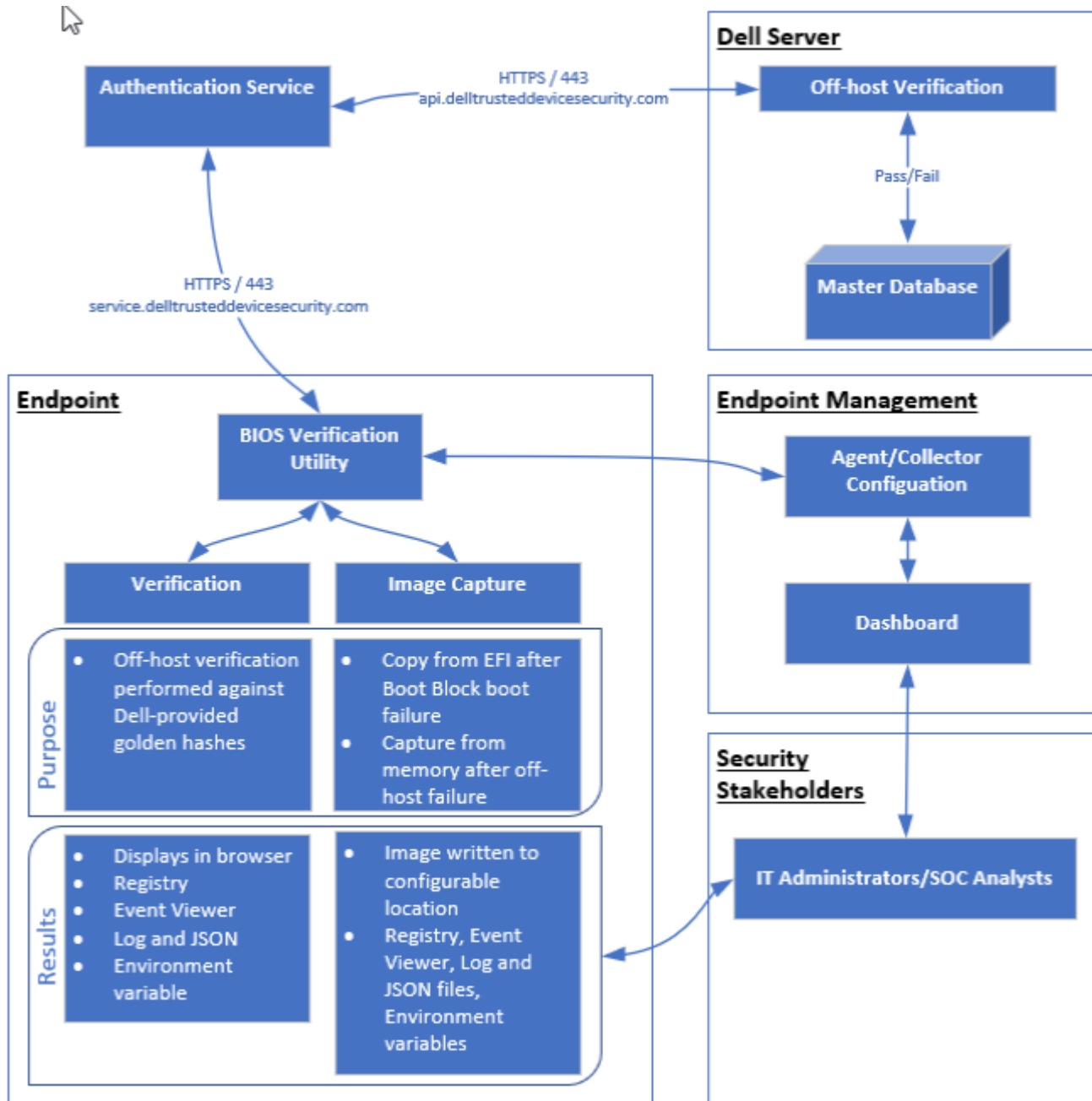
- The following table details supported operating systems.

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

- Windows 10

Architecture

The following diagram illustrates BIOS Verification architecture. For a list of Dell computer models supported with BIOS Verification, see [Requirements](#).




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.

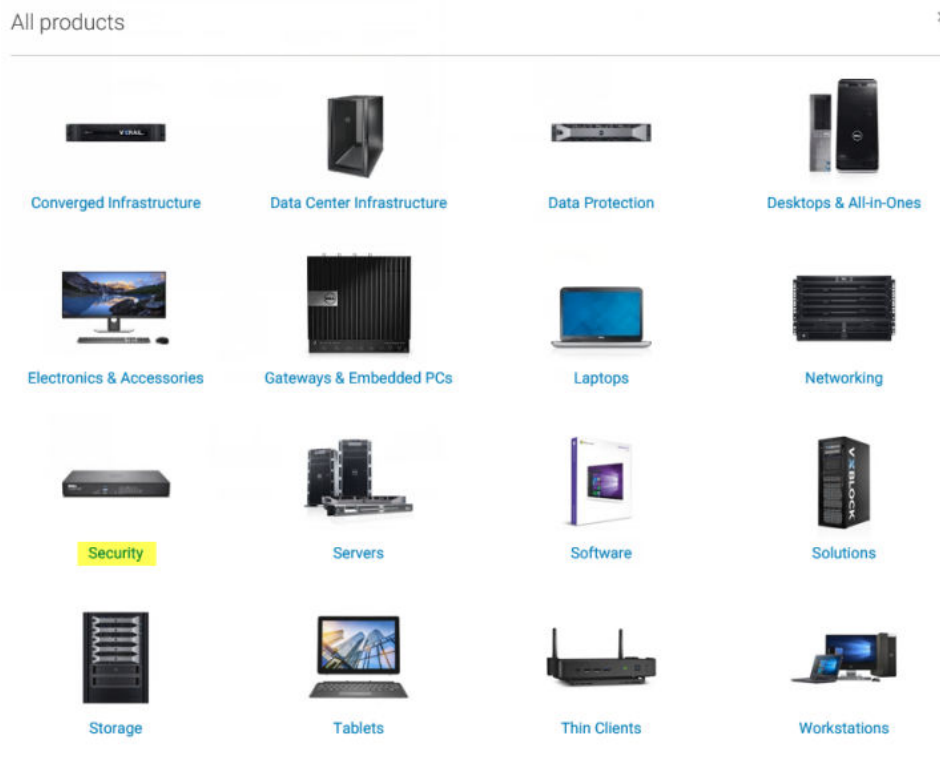
1. On the Dell Support webpage, select **Browse all products**.

Enter a Service Tag, Serial Number, Service Request, Model, or Keyword. **i**

What can we help you find?  or [Detect PC](#)

[Browse all products](#) [Find my Dell EMC Product](#)

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



3. Select **Trusted Device Security**.

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

Dell Data Security

Trusted Device Security

- 4. Select the product.
BIOS Verification
- 5. Select **Drivers & downloads**.
- 6. Select the desired client operating system type.
- 7. Select **BIOS Verification**.

OVERVIEW DRIVERS & DOWNLOADS DOCUMENTATION

Find a driver for your BIOS Verification

Keyword: Operating system:

Category: Format:

Show urgent downloads only

NAME	CATEGORY	RELEASE DATE	ACTION
<input type="checkbox"/> BIOS Verification Utility	Trusted Device Security	04 Sep 2019	<input type="button" value="Download"/>

- 8. Select **Download**.

Download

Installation

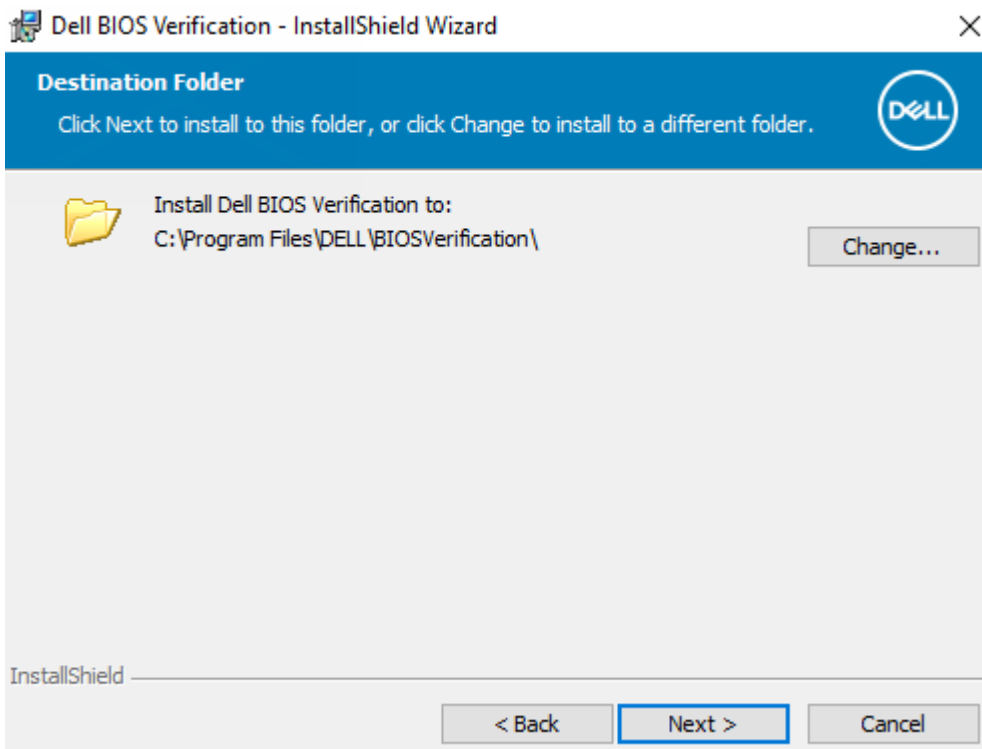
Use one of the following methods to install the utility:

- Interactive Installation
- Command Line Installation

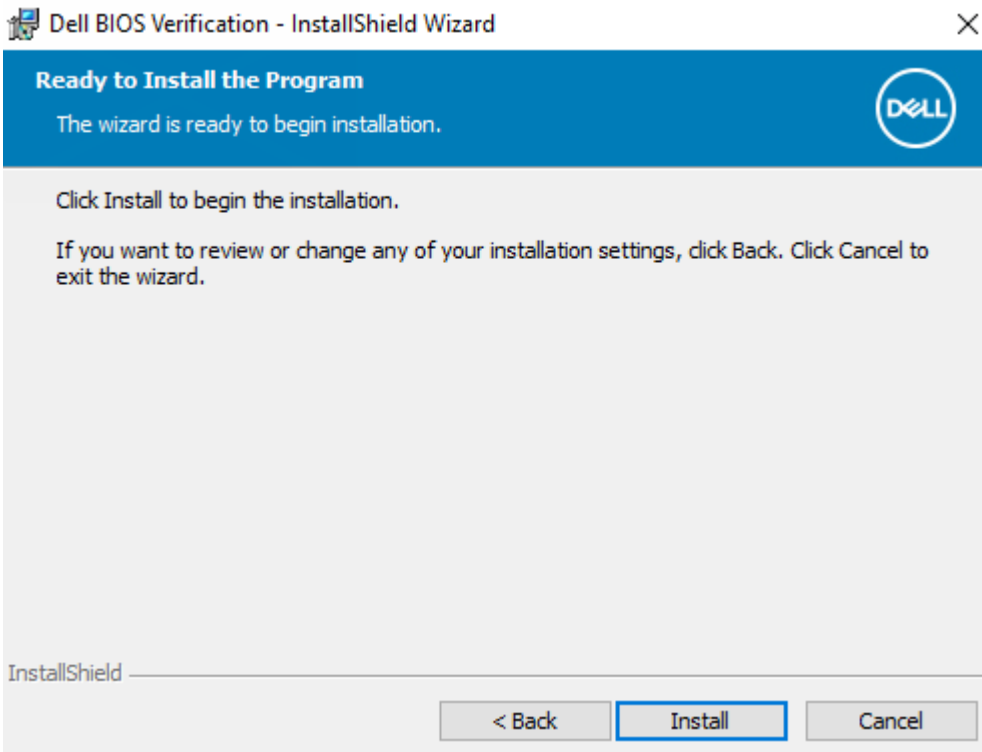
Interactive Installation

The BIOS Verification installer requires administrative rights. The bit-rate of the utility must match the architecture of the host computer's operating system. Choose one of the following:

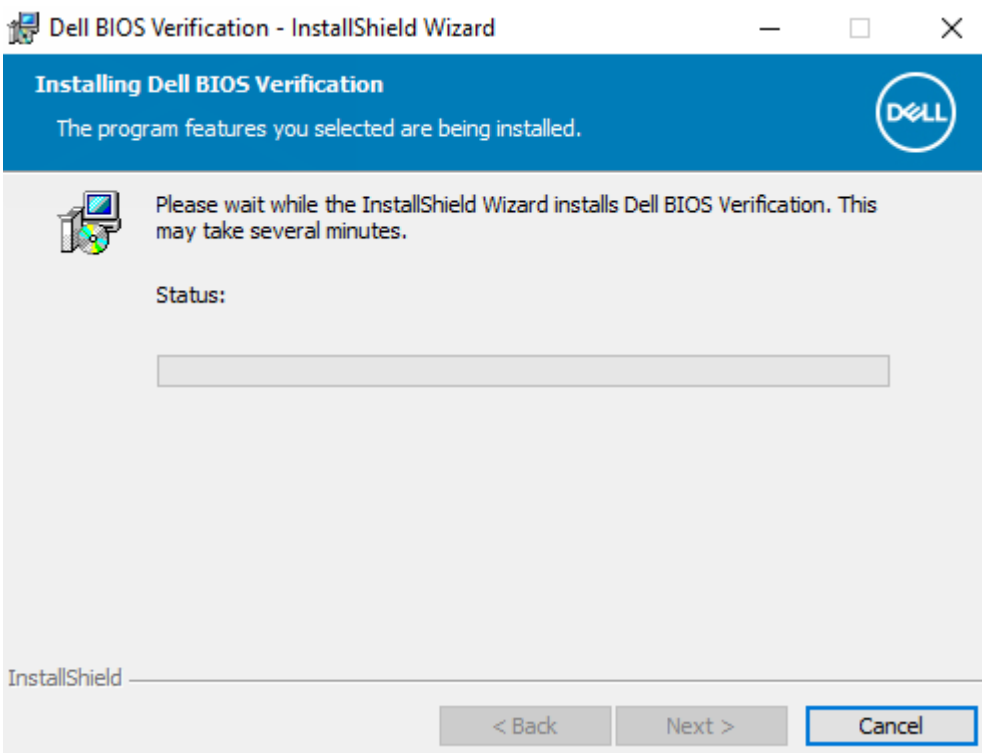
- BIOSVerificationSetup.exe - 32-bit installer
 - BIOSVerificationSetup-64Bit.exe - 64-bit installer
1. Copy **BIOSVerificationSetup-64Bit.exe** to the local computer.
 2. Double-click **BIOSVerificationSetup-64Bit.exe** to launch the installer.
 3. Click **Next** at the Welcome screen.
 4. Read the license agreement, agree to the terms, and click **Next**.
 5. Click **Next** to install the utility in the default location of C:\Program Files\Dell\BIOS Verification\.



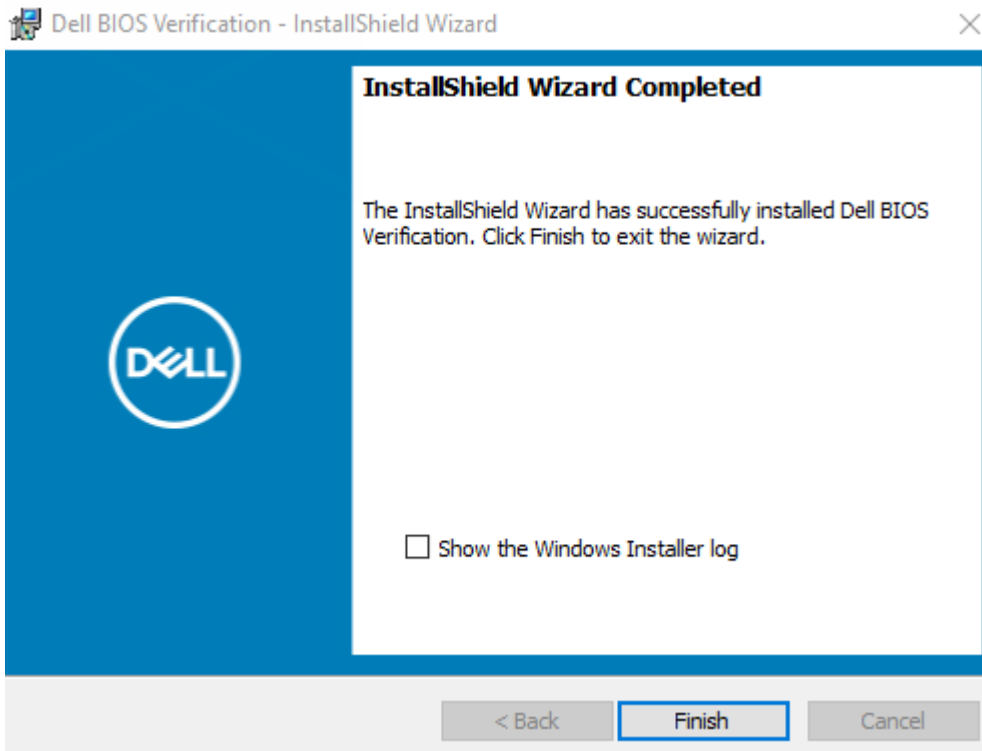
6. Click **Install** to begin the installation.



7. A status window displays. This takes several minutes.



8. Click **Finish**.



BIOS Verification Installation is complete.

After installation, a browser launches and displays results. See [Results, Troubleshooting, and Remediation](#) for more information.

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 installers to install the utility 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%, located at C:\Users\\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 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 BIOS Verification Utility

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

- BIOS VerificationSetup.exe - 32-bit installer
- BIOS VerificationSetup-64Bit.exe - 64-bit installer
- The following example installs the 32-bit BIOS Verification utility with silent installation, no progress bar, installed in the default location of **C:\Program Files\Dell\BIOS Verification** and installation logs in **C:\Dell**.

```
BIOSVerificationSetup.exe /s /qn /l*v C:\Dell\BIOSVerification.log
```

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

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

Deployment and Collection

When installing BIOS Verification with third-party utilities, Dell recommends targeting 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 Microsoft's 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 Microsoft's SCCM based on generated collections. For more information on generating deployment tasks and scheduling across larger environments, see <https://docs.microsoft.com/en-us/sccm/apps/deploy-use/deploy-applications>.

Additional third-party utilities use similar 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>.

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

Uninstall BIOS Verification

The user performing uninstallation **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 BIOS Verification** then left-click **Uninstall**.

Uninstall from the Command Line

The following example uninstalls BIOS Verification:

```
wmic path win32_product where (Caption like "Dell BIOS Verification") call uninstall
```

Image Capture

Administrators can capture images of corrupted or tampered BIOS for analysis and remediation. When run, BIOS Verification 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\BIOSVerification\ImageCapture. Additionally, BIOS Verification copies corrupt or tampered images from memory to %PROGRAMDATA%\Dell\BIOSVerification\ImageCapture if off-host verification fails.

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 if copied from the EFI partition and BIOSImageCaptureBVSMMDDYYYY_HHMMSS.bv if copied from memory. MMDDYYYY is the date and HHMMSS is the time of image copy. For Command Line parameters, see the [Run the Utility](#).

For more information on Image Capture and the Windows Registry, see [Results, Troubleshooting, and Remediation](#).

Run the Utility

Use one of the following methods to run the utility:

- Interactively
- Command Line

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

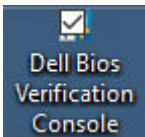
NOTE: BIOS Verification determines Dell platform support at runtime.

Run the Utility by Schedule

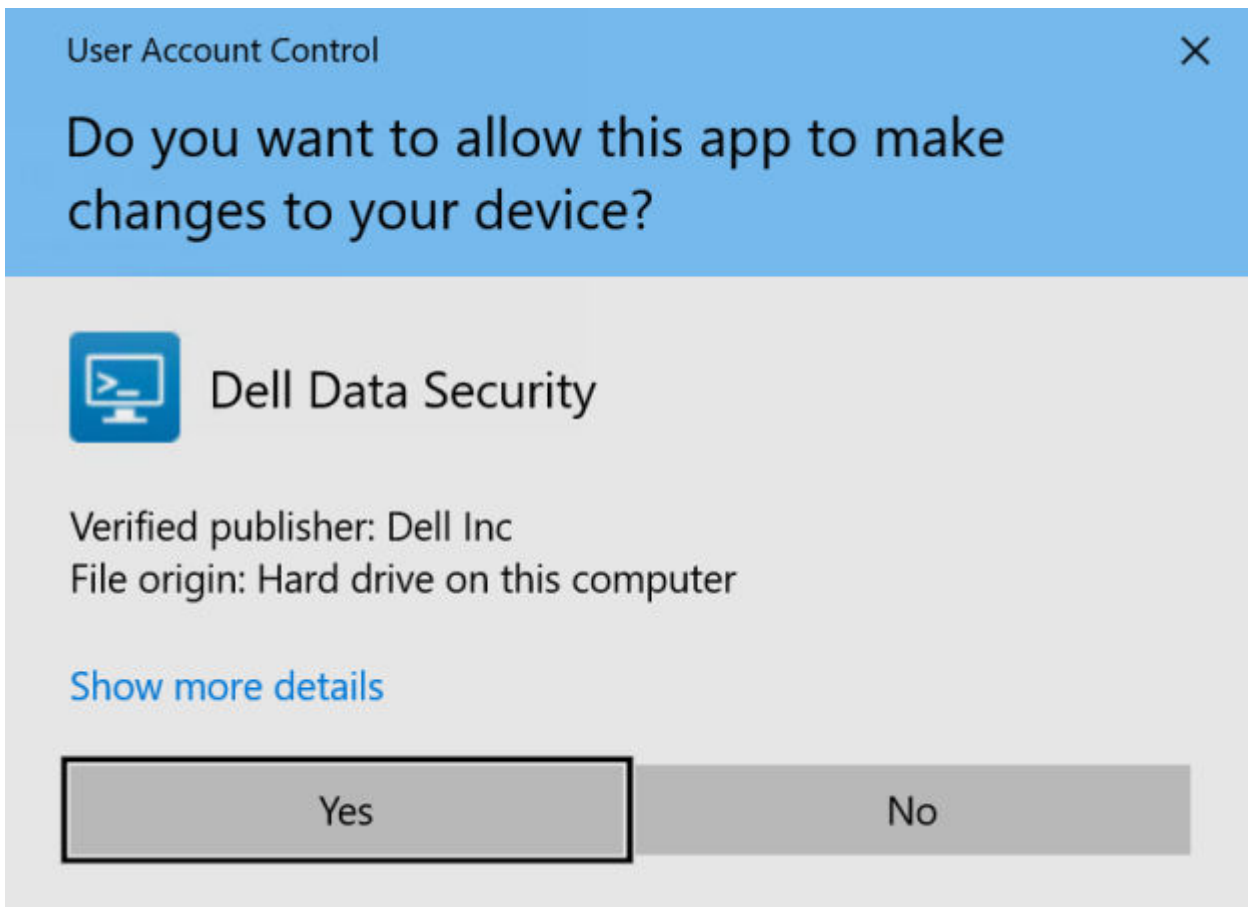
To schedule BIOS Verification to run at set intervals or to trigger execution by events, refer to Microsoft Task Scheduler documentation [here](#).

Run the Utility Interactively

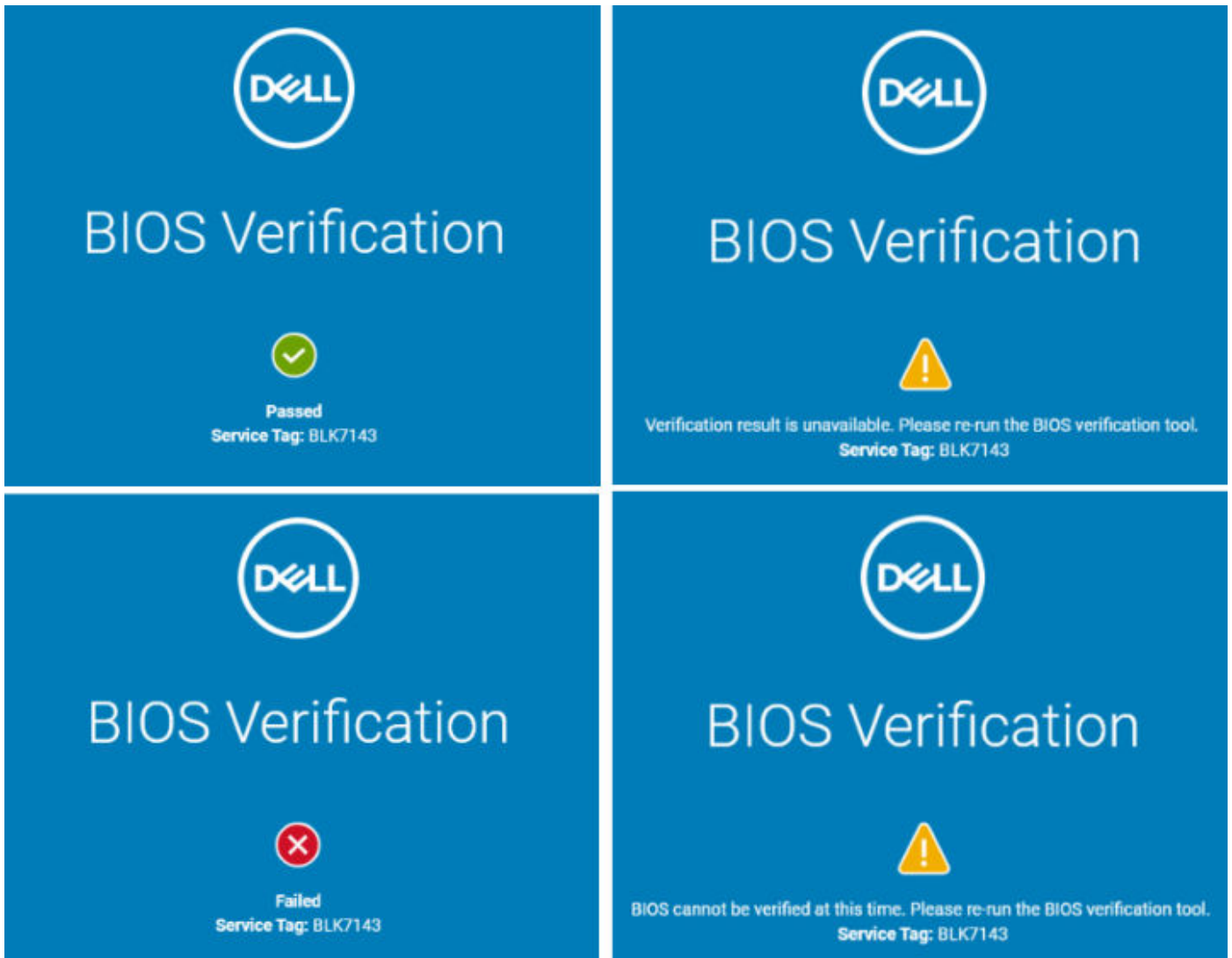
1. Double-click **Dell BIOS Verification Console**.



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 Utility 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, 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. Navigate to the directory containing the utility
3. Type **Dell.SecurityCenter.Agent.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.SecurityCenter.Agent.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 BIOS Verification in repeated intervals ensures devices remain in a protected state. Third-party utilities are commonly used to run and report back on a schedule. Dell Recommends targeting specific collections of devices to avoid a high volume of noise from unsupported platforms.

Dell recommends running BIOS Verification with its headless property as SYSTEM on devices to avoid interrupting users while ensuring the proper return codes.

- The following example runs BIOS Verification in headless mode with logs and results written to the default location of `C:\ProgramData\Dell\BIOSVerification\`:

```
C:\Program Files\Dell\BIOS Verification\Dell.SecurityCenter.Agent.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](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 BIOS Verification, Dell recommends 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>.

Results, Troubleshooting, and Remediation

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

Results

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

%PROGRAMDATA%

BIOS Verification writes logs and JSON formatted results to C:\ProgramData\Dell\BiosVerification\.

%ERRORLEVEL% Environment

BIOS Verification writes pass/fail results to the %ERRORLEVEL% environment. After running the utility, 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

BIOS Verification writes a new notification to the Event Viewer each run. Find these notifications in Event Viewer under **Application and Service Logs > Dell** with Source type **BiosVerification**. The following table details the BIOS Verification events in Event Viewer. The following table details Event Viewer notifications after running BIOS Verification or Image Capture.

Action	Level	Event ID	Task Category
Verification Passed	Information	1	None
Verification Failed	Error	1	None
Image Captured	Warning	1	2
Duplicate Image Capture	Warning	2	2
No Image Found	Informational	3	2

Registry

BIOS Verification results are written to the registry each time the utility is run. All BIOS Verification and Image Capture related registry keys are located at HKLM\Software\Dell\BiosVerification.

Off-host Verification

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

HKLM\Software\Dell\BiosVerification

Result.json

True=Pass

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\BiosVerification
"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\BiosVerification
"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
- A private key used to verify 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.

Troubleshooting

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 BIOS Verification again. If this error persists, reinstall BIOS Verification or contact Dell Support.
3	An unknown error occurred	BIOS Verification detail retrieval failed. Please run BIOS Verification again. If this error persists, contact Dell Support.
4	An invalid command line argument was specified	A command line variable passed to BIOS Verification is not supported. Please see the supported command line syntax for BIOS Verification here or run BIOS Verification with the <code>-help</code> switch or <code>/?</code>
5	The utility is running with insufficient privileges	BIOS Verification requires local administrator rights to run.
6	An internal error has occurred	An error on the local device occurred preventing BIOS Verification from properly running. Run BIOS Verification again. If this error persists, contact Dell Support.
7	Server responded with an error or is unavailable	The BIOS Verification server is unavailable. Validate network connectivity and that the web-based locations are accessible from the device.

Error Code	Meaning	Additional Information
8	An issue in the driver occurred	BIOS Verification'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 <code>-help</code> command line argument is specified	BIOS Verification was run with the <code>-help</code> argument.
11	This is returned if the platform or BIOS image is not supported	BIOS Verification 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.

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.