Dell SafeBIOS with Modern Management

By Sven Riebe, Dell MCSG Technical Architect team

Edited by

Gus Chavira, Dell MCSG Technical Architect team and

Amy Price, Dell MCSG Evangelist

Client Security in a Hybrid working world: is it even possible to be safe?

"There is no 100% certainty, but we can achieve a lot by using all the means at our disposal."

Over the past three decades, we've seen PC's move from the land of hobbyists into their role today as an essential business tool. But ever since there was a PC, there was someone trying to do something malicious with them, and antivirus technology had to become substantially more sophisticated to keep pace with both technology waves and hacker innovations.

Originally antivirus worked in a standalone manner, checking the device on demand in a batched/scheduled mode. In 1998, one of the first true self-propagating viruses (the I Love You virus) created a huge challenge for IT departments, bringing the need for a solid cybersecurity defense to the forefront. As a result, organizations started to invest in security based upon real time incidents, and antivirus became a standard requirement.

Hackers are creative by nature and are constantly developing new methods of attack, ranging from email attachments to complex network hacks and social engineering. Client devices provide a virtual petri dish for the incubation and propagation of new and sophisticated attacks (at least five of the nine Initial Access points in the MITRE ATT&CK Framework are client device-based), and maintaining security also requires companies to invest in technologies like VPN (Virtual Private Network), Firewalls and NAC (Network Access Control). As attack methods rapidly change, IT organizations find themselves in a constant state of analysis, evaluation and deployment of defenses to protect their environment and secure IT infrastructure and devices.

Hardware and silicon chips can also be affected by security issues – the Meltdown/Spectre vulnerability was one of the most impactful examples of this. Chip and software vendors as well as equipment manufacturers have adopted secure development and supply chain security processes to help defend against intrusions into their products, but it still represents an area of vulnerability to what we call "below the OS (Operating System)" attacks. Today Dell is using technologies which provide hardware-based security (like TPM (Trusted Platform Module)) but these defenses require that the OS trusts the chips.

More recently, we've seen attacks directly on BIOS and firmware as well. In 2019, Dell released SafeBIOS (Aka Trusted Device Agent) to help IT departments comprehend the security status of their client hardware and act accordingly. This article will address Dell SafeBIOS features and how these capabilities can facilitate and augment overall security posture holistically. Dell has long taken the position that continually evolving security defenses is the best offense against future attack, and SafeBIOS is a framework that is continually updated with the latest protections for Dell client devices.

In our engagements with IT departments over the years, we've learned that it's not enough to simply have great cyber defences: it's also a requirement that they be manageable by IT. Security Operations (SecOps) become involved when an attack is detected, but the day-to-day operation of cyber security in an organization is the responsibility of IT. In this article, we'll discuss not only what SafeBIOS is, how it works and what capabilities it brings to Dell endpoints – we'll also address some of the ways in which SafeBIOS has been integrated into the flow of client management tools to ensure that Dell devices have the latest defenses, continually updated.

What is Dell SafeBIOS?

Modern security solutions are fulfilling their role to check the OS and the Secure Boot of the machine, but how does that work if the BIOS itself is compromised or vulnerable? Dell SafeBIOS, now named in the download section as Dell Trusted Device Agent https://www.dell.com/support/home/en-us/product-support/product/trusted-device/drivers, is the missing piece in an overall security management strategy to protect against hardware and 'below the OS' threats.

First, Dell SafeBIOS does an 'off-host' verification check against a secure cloud database hosted by Dell. All Dell PC clients run this at startup or at most every 12 hours. The client gets a result of verification positive or negative. You might be asking why we do an off host or cloud-based check and not on the local device himself. That´s a good question, and the value of this implementation is that:

1. **No specific chip is needed on the device**, making this solution simple to use and supportable on older devices as well. Supported Platforms: https://www.dell.com/support/manuals/en-us/trusted-device/trusted_device/platforms?guid=guid-b5a91b49-429a-4a97-b4fb-5bf67c67098a&lang=en-us
2. **There are multiple points of contact**, so hackers would need to afflict the device AND the secure cloud data base which would make it more difficult to compromise (implementing a kind of login MFA (Multi Factor Authentication) – to secure the device).

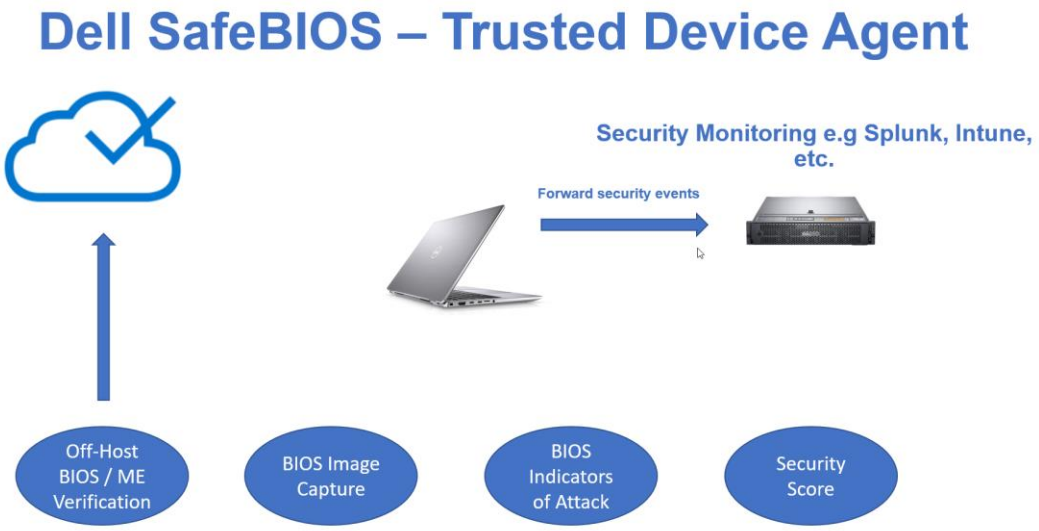
Though a fully PC hosted solution may be preferred, the value of a solution like SafeBIOS is to secure the BIOS before the OS is started. We are expecting to see increased attacks on these below the OS components in future.

An example of a similar strategy is Microsoft using UEFI (Unified Extensible Firmware Interface) Trusts to update firmware in Windows updates. If this method is compromised by malware, then the process to address it would roll out through Windows Update and spread quickly. Though there are quality checks, a 100% guarantee of security is not possible, as evidenced by the example of the SolarWinds issue where various companies were affected.

Most organizations have embraced an approach of 'security in layers' to defend against cyber-attacks, with the belief that if an attack makes it through one defense, there are others to help stop it. Dell SafeBIOS is an added solution which enhances security posture in conjunction with other solutions like next generation virus scan and advanced threat protection software, firewalls, email anti-phishing tools and even security training.

What are the Features of Dell SafeBIOS?

1. **Off-Host BIOS Verification** (at startup or every 24 hours)
   Off-host BIOS Verification uses a secure cloud environment to conduct a "point in time" check for the integrity of the BIOS.
2. **BIOS Image Capture** (for forensic data if needed)
   If a BIOS appears compromised, the BIOS image is captured for forensic analysis.
3. **BIOS Indicators of Attack**
   With over 300 BIOS configurations possible, which may appear like normal administrative actions, an attack could easily go undetected. With BIOS Indicators of Attack (IoA), attacks or suspicious actions are identified, and the IT administrator is alerted.
4. **Dell Safe BIOS Security Score** (additional to Microsoft Security Center incl. BIOS Password status, Indicators of Attack as well)
   The score is a value between 0 and 100 based on the following factors: BIOS Password, BIOS Verification, Firewall status, Virus-Scanner status, Intel ME (Manageability Engine), Disk encryption and Indicators of Attack (BIOS settings)
5. **Intel ME Verification**
   The Trusted Device agent scans and verifies that Intel ME firmware is present and untampered after initial installation, startup, and every 24 hours.



How to acquire and install this software in an enterprise environment

The Dell SafeBIOS software supports all Dell commercial business platforms: OptiPlex, Latitude, Precision and XPS mobile devices (note that old generation Dell PCs may not have support for Dell SafeBIOS: https://www.dell.com/support/manuals/en-us/trusted-device/trusted_device/platforms?guid=guid-b5a91b49-429a-4a97-b4fb-5bf67c67098a&lang=en-us).

If you are looking for SafeBIOS in the download section, please note SafeBIOS is branded as Dell Trusted Device Agent.

Download Link:

https://www.dell.com/support/home/de-de/product-support/product/trusted-device/drivers

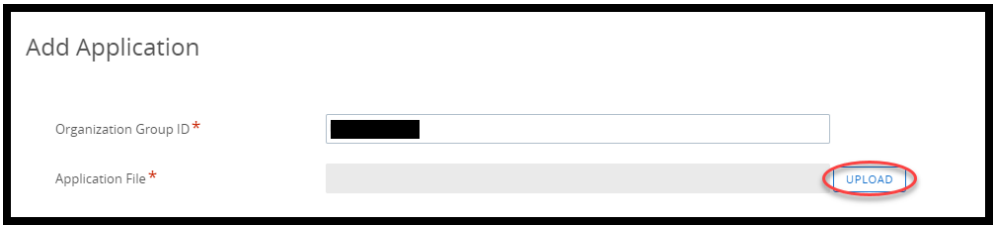
Documentation:

https://www.dell.com/support/home/de-de/product-support/product/trusted-device/docs

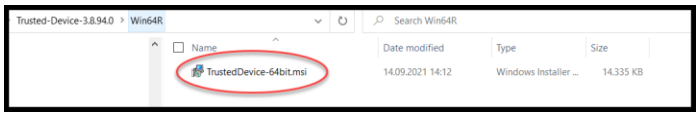
The Zip-File includes an MSI, making it easy to install this agent with your existing Software Distribution Platform like, SCCM (System Center Configuration Mgr), Workspace One UEM (Unified Endpoint Management) or another solution. Our example covers the delivery of this software with VMware Workspace One UEM. This process is similar if you are using other UEM software management tools.

Example software delivery with VMware Workspace One UEM

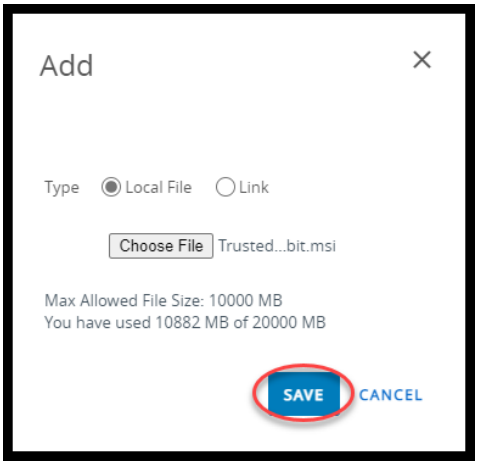
Select to add a new application in the Workspace One UEM console



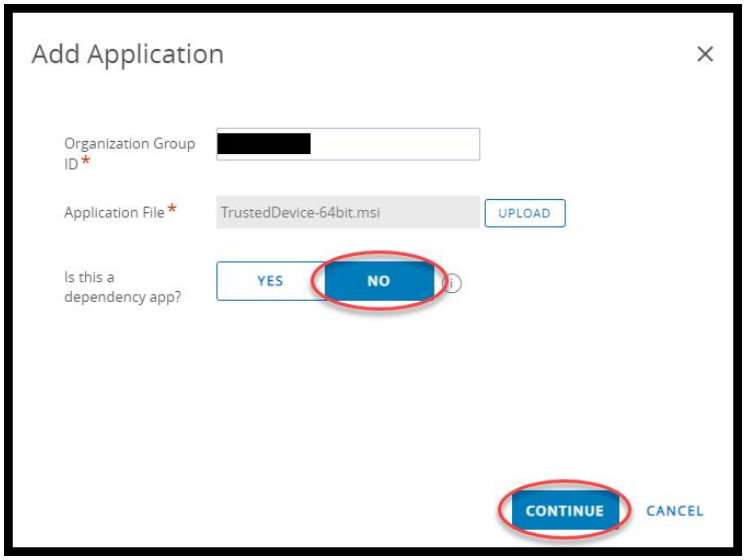
You have 32 and 64-Bit options of MSI-File. This example uses the 64-Bit Version of Trusted Device Agent.



Upload the MSI to the repository.



Accept the default values here.



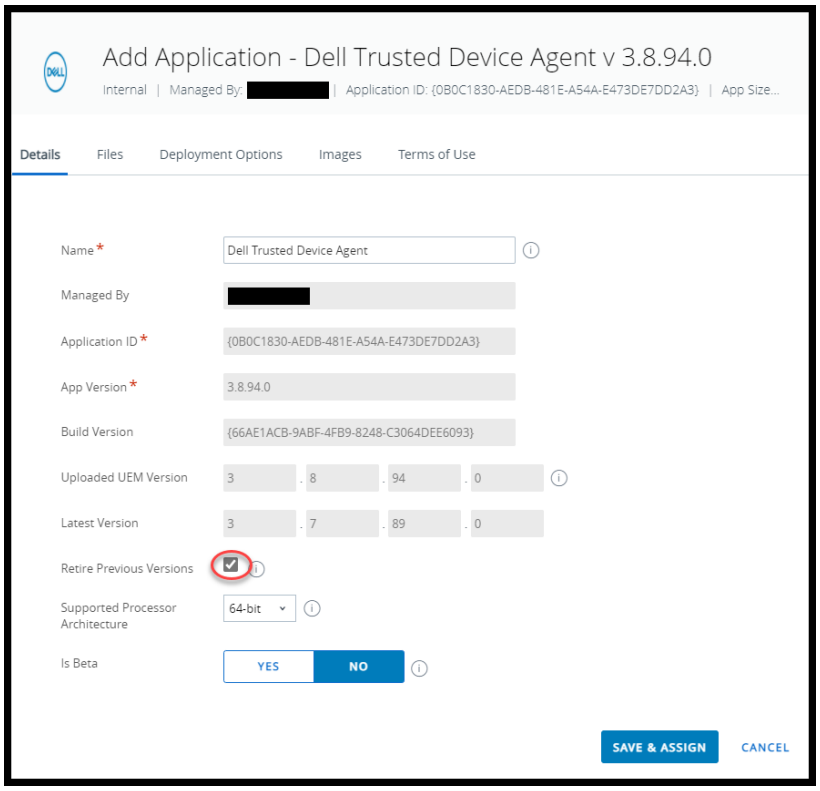
If you have completed the upload of the MSI, all the required fields are filled in automatically. If you have an older version in place, you could enable the retirement of previous versions. Otherwise, you will have different versions of this agent in place, which could cause issues.

Section ‘Details’

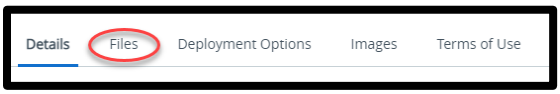
No changes

Field	Value
Retire Previous Versions	☑

Note: This option is only available if an older deployment package is still active.


Add Application - Dell Trusted Device Agent v 3.8.94.0
Internal | Managed By: [redacted] | Application ID: {0B0C1830-AEDB-481E-A54A-E473DE7DD2A3} | App Size...
Details
Files
Deployment Options
Images
Terms of Use
Name *
Dell Trusted Device Agent
Managed By
[redacted]
Application ID *
{0B0C1830-AEDB-481E-A54A-E473DE7DD2A3}
App Version *
3.8.94.0
Build Version
{66AE1ACB-9ABF-4FB9-8248-C3064DEE6093}
Uploaded UEM Version
3 . 8 . 94 . 0
Latest Version
3 . 7 . 89 . 0
Retire Previous Versions
Supported Processor Architecture
64-bit
Is Beta
YES
NO
SAVE & ASSIGN
CANCEL

Section ‘Files’



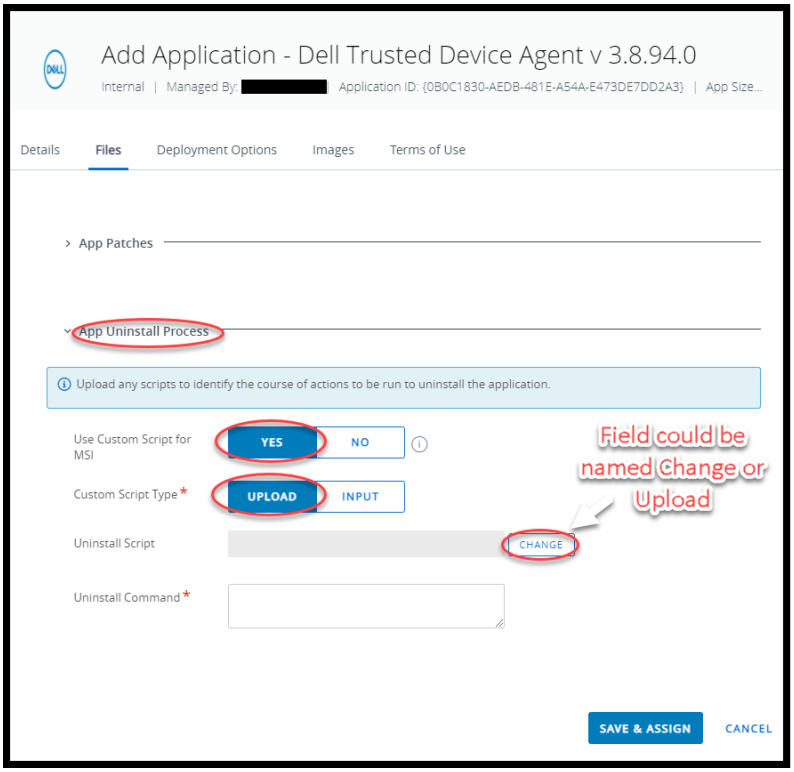
Add an uninstall script for Dell Trusted Device Agent.

Section ‘App Uninstall Process’

Field	Value
Use Custom Script for MSI	Yes
Custom Script Type	Upload

Click ‘Upload or Change’

Note: The field is first called ‘Upload’ and later when changes are made to the software package ‘Change’



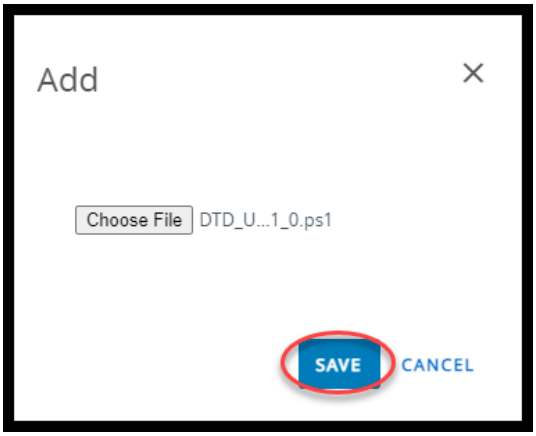
Generate an uninstall script **DTD_Uninstall_V1_0.ps1**

```
$App = Get-WmiObject -Class win32_product -Filter "Name like '%Dell Trusted Device%'" | select -ExpandProperty IdentifyingNumber
msiexec.exe /x "$App" /qn REBOOT=R
```

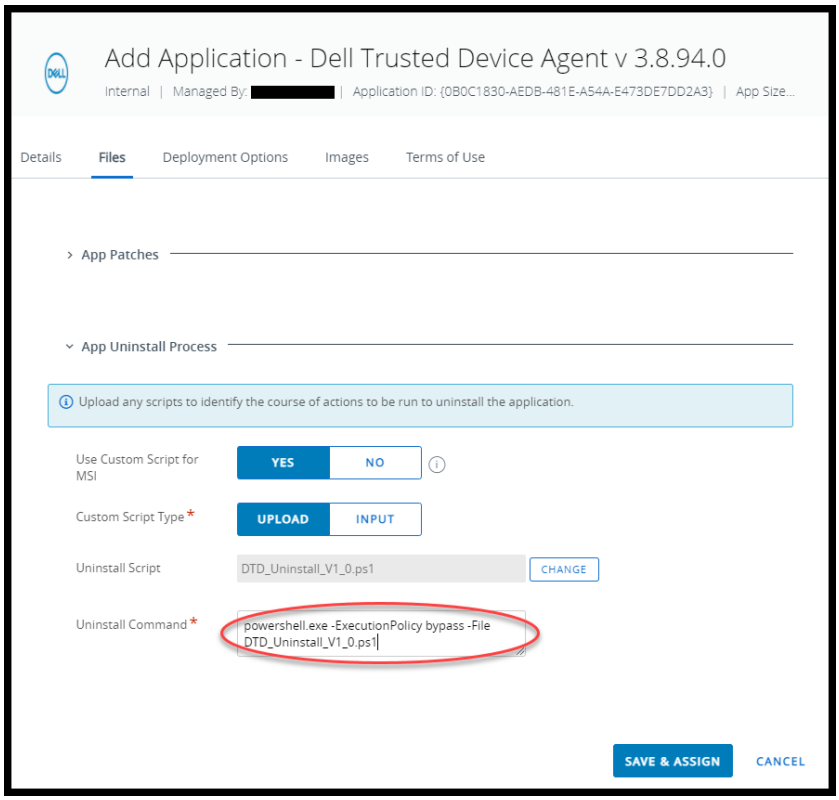
Value REBOOT=R suppressing the Reboot, which normally is **immediate.**

Choose the uninstall script, e.g., **DTD_Uninstall_V1_0.ps1**

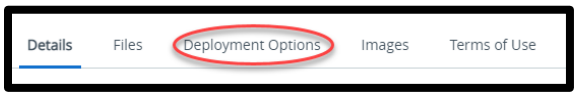
Click ‘Save’



Field	Value
Uninstall Command	powershell.exe -ExecutionPolicy bypass -File DTD_Uninstall_V1_0.ps1



Section ‘Deployment’

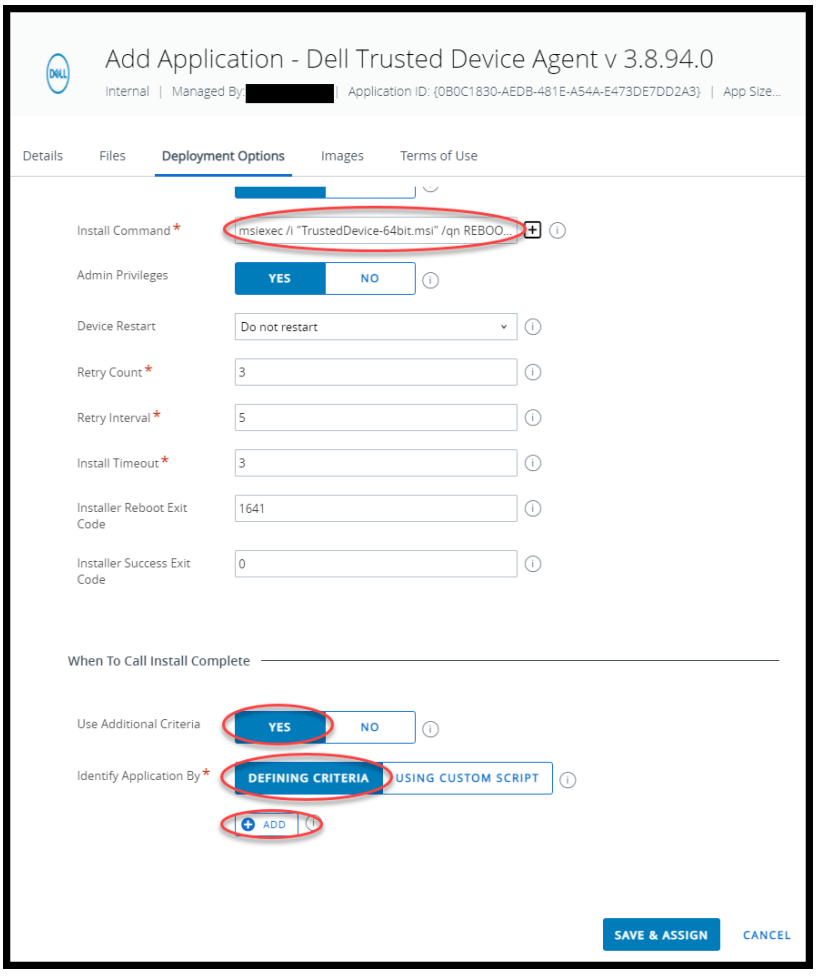


Field	Value
Install Command	msiexec /i "TrustedDevice-64bit.msi" /qn REBOOT=ReallySuppress

Section ‘When to Call Install Complete’

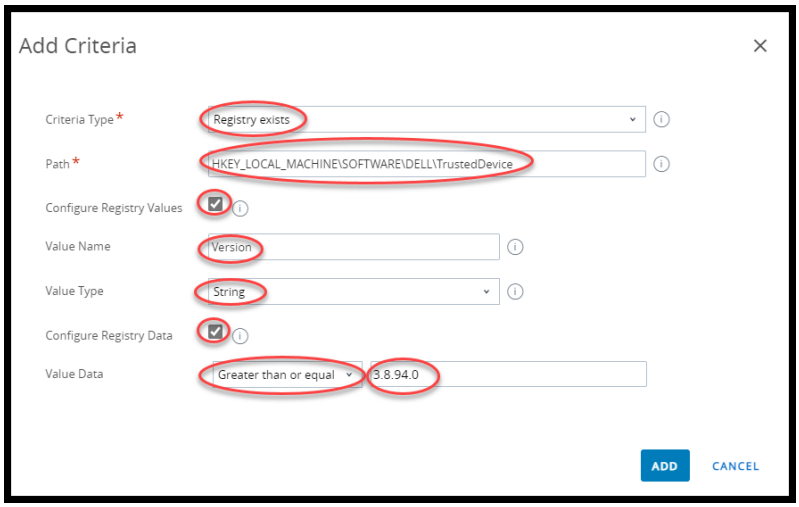
Field	Value
Use Additional Criteria	Yes
Identify Application By	Defining Criteria

Click ‘Add’

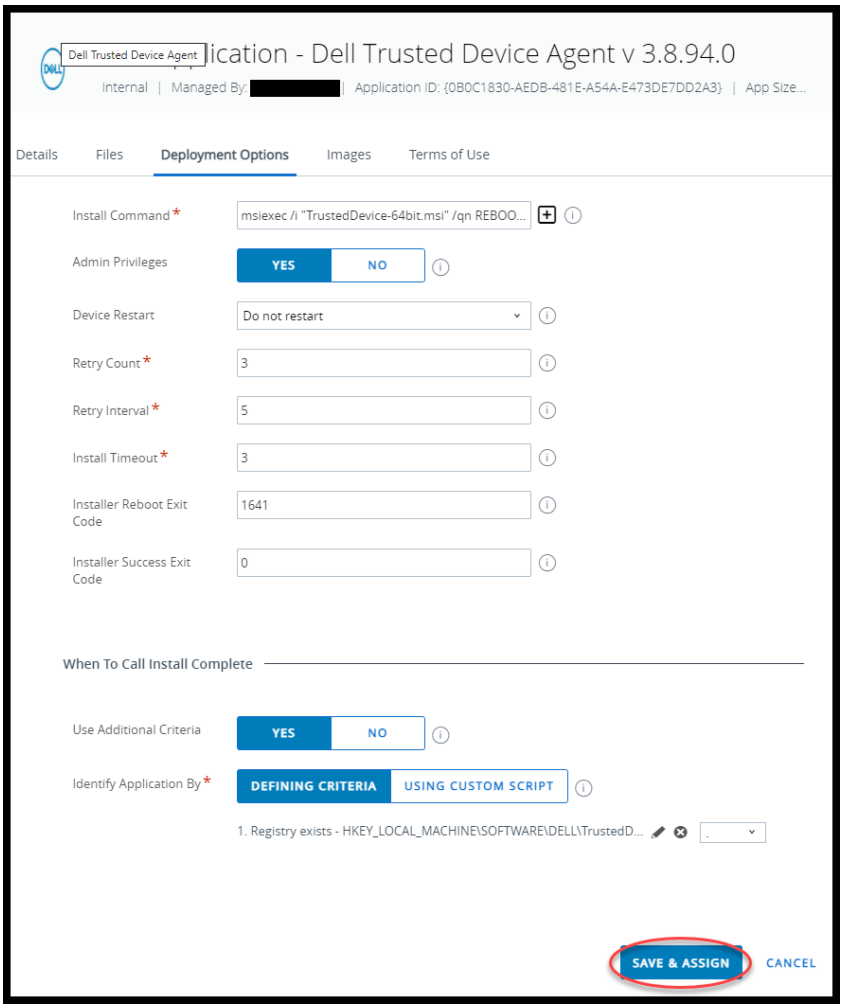


Section ‘Add Criteria’

Criteria Type	Registry exists
Path	HKEY_LOCAL_MACHINE\SOFTWARE\DELL\TrustedDevice
Configure Registry Values	☑
Value Name	Version
Value Type	String
Configure Registry Data	☑
Value Data	Greater than or equal 3.8.94.0 (Note: use version of Trusted Device)



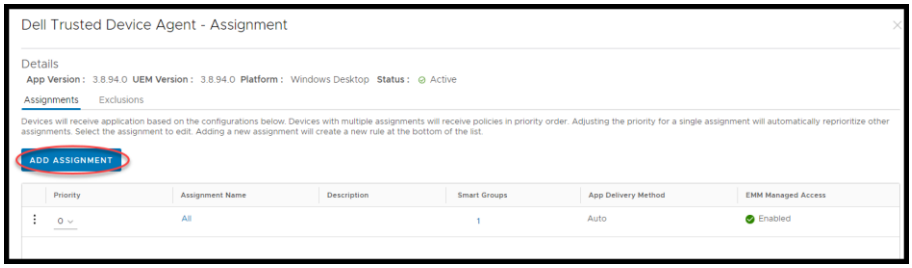
Click ‘Save & Assign’



Section ‘Assignment’

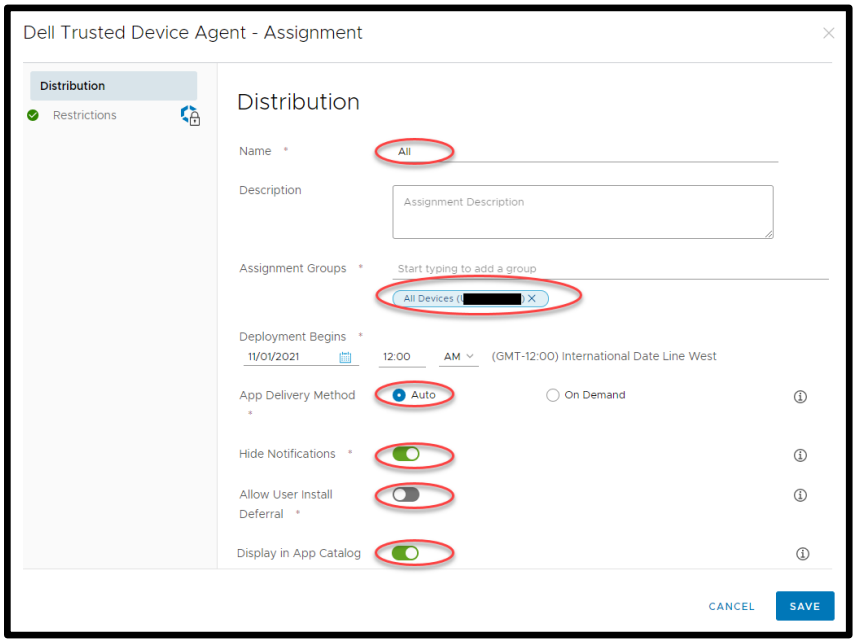
Click ‘Add Assignment’

Note: Add Assignment opens automatically if the Application is uploaded for the first time.



Section ‘Distribution’

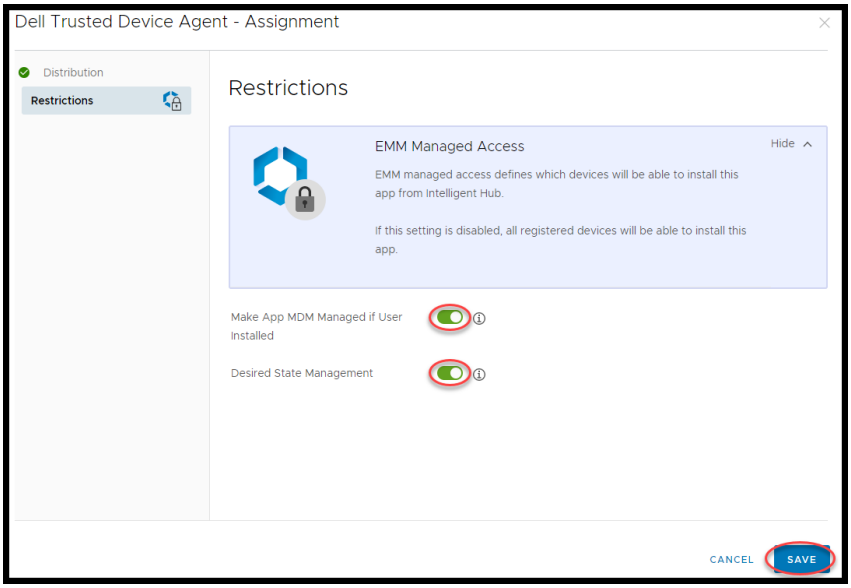
Field	Value
Name	like All Dell Device (helps to better identify the assignment)
Assignment Groups	Dell Trusted Device Agent supports only Dell devices (Latitude, Optiplex, Precision and mobile XPS), it makes sense to have a dynamic smart group which includes these devices only.
Deployment Begins	When you plan to deploy this application
App Delivery Method	Auto
Hide Notification	On (This tool is only for admins relevant)
Allow User Install Deferral	Off (Security Software should be installing every time)
Display in App Catalog	Off



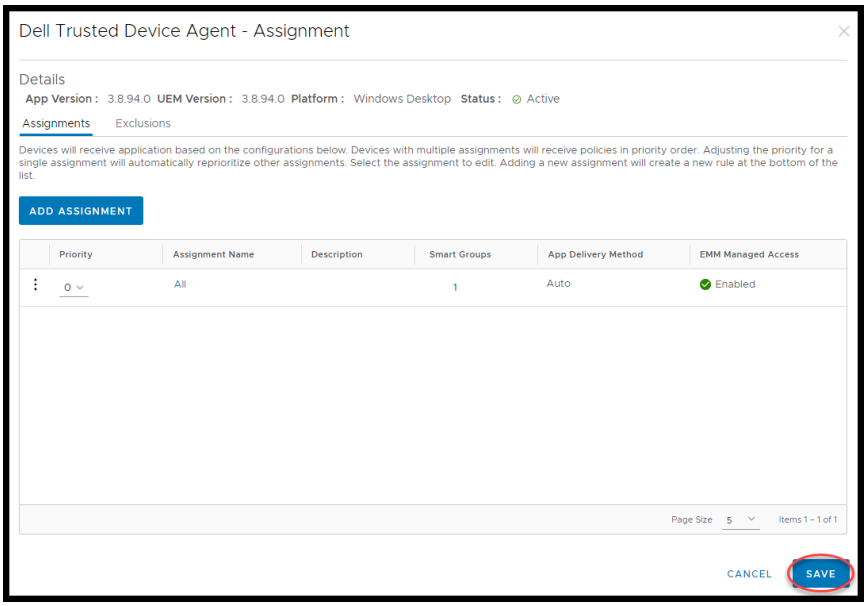
Section ‘Restrictions’

Field	Value
Make App MDM Managed if User installed	On (now all installation will be managed by IT)
Desired State Management	On (if User has Admin rights and uninstall this App, the app will be reinstalled directly by Workspace One)

Click ‘Save’

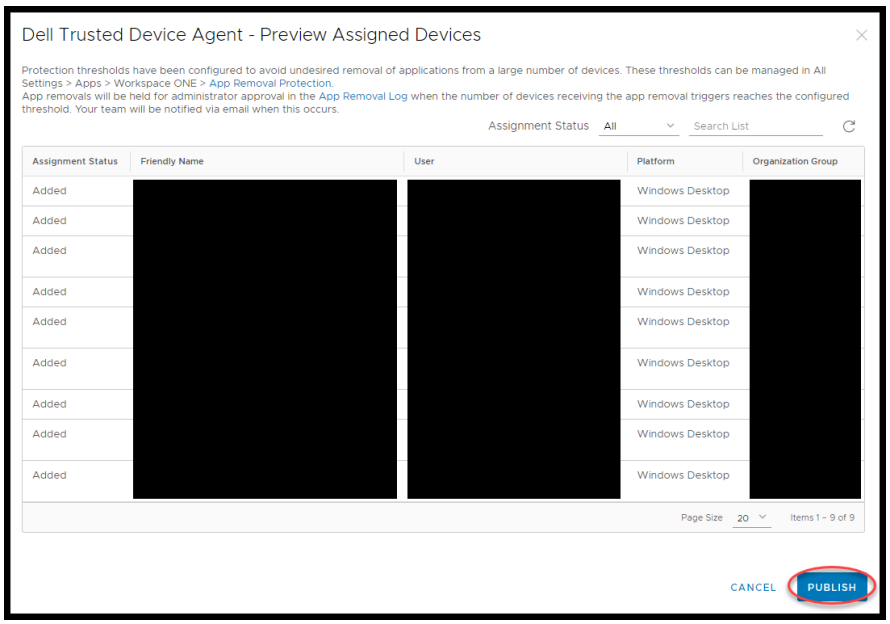


Click ‘Save’

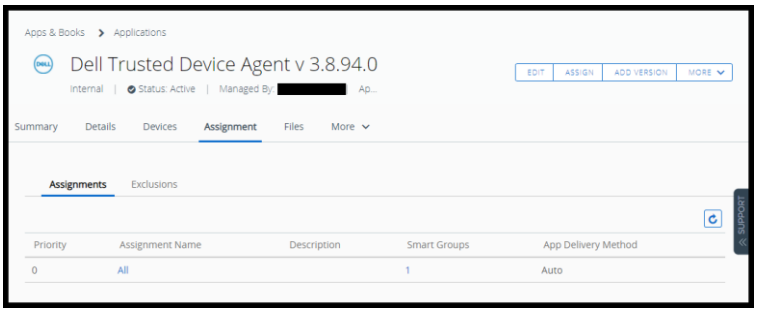


Cross check to ensure that this assignment matches to the correct devices.

Click ‘Publish’.



Ready to work.



System Management with Dell SafeBios

User interface

Dell SafeBIOS has options on how it provides BIOS verification. The easiest way is directly to the user on the device itself. The end-user or admin in a remotely connected session can start the agent software to query the BIOS status, and feedback is received and displayed through a browser window.

Command Line

Dell SafeBIOS has a CLI (Command Line Interface) interface as well. If you started the Dell.TrustedDevice.Service.Console.exe with /headless option, you would receive the result of BIOS Verification only as CLI output.

```
C:\Program Files\Dell\TrustedDevice>Dell.TrustedDevice.Service.Console.exe /headless
BIOS Verification: 0 (Success)
```

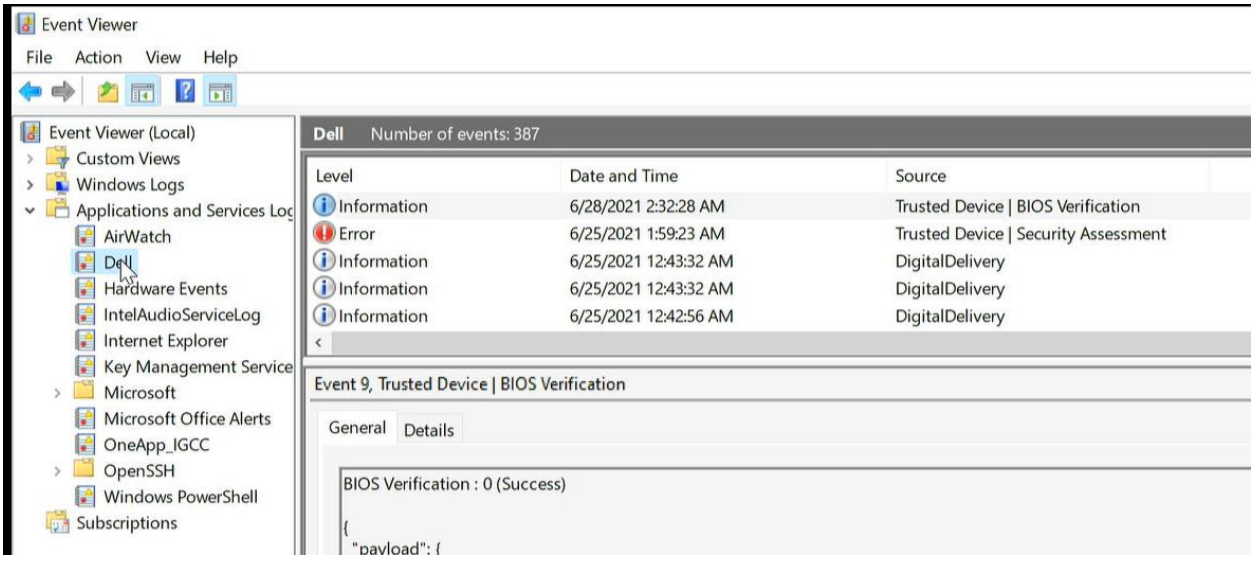
The CLI interface also has a couple of other options like the export of the UEFI in case you need this for a further forensic analysis.

```
C:\Program Files\Dell\TrustedDevice>Dell.TrustedDevice.Service.Console.exe /?
Usage: Dell.TrustedDevice.Service.Console.exe [options]

Options:
  -?|-help           Show help information
  -noncefile         Use the nonce in the specified command line
  -noncestring       Use the nonce specified by the Base64 string
  -export            Image Capture Only: Export latest stored image to the specified path
  -updateimagestore  Update the configured Captured Image Store location
  -headless          Runs application without a GUI (does not open browser with result)
  -exportall         Image Capture Only: Exports all stored images instead of the latest
  -imagecapture      Run BIOS image capture instead of BIOS verification
```

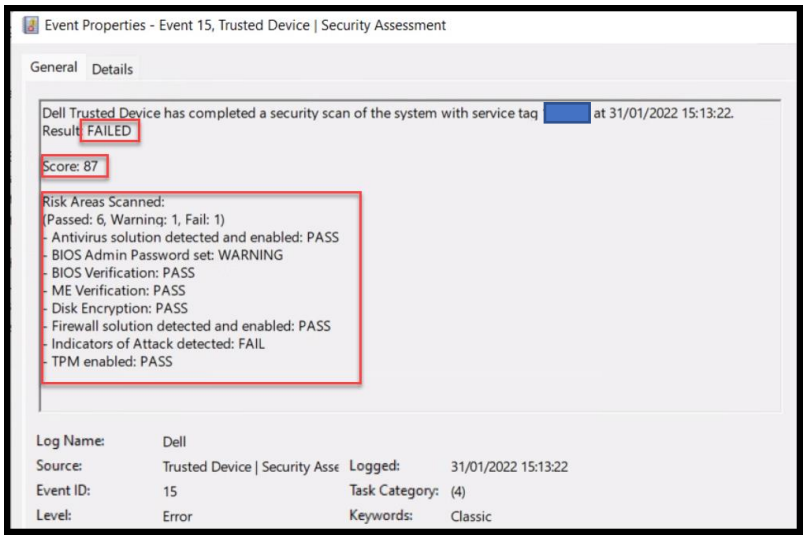
Microsoft Event Viewer

Dell SafeBIOS writes events in the Microsoft event logs. These events provide the IT admin with more detailed information about BIOS verification, the device's Security Score and notification about any detected Indicators of Attack. Microsoft events can also provide this information to other management tools in use. We show later how this information may be incorporated and integrated into a modern management solution like Workspace One UEM. (Please note that Microsoft Intune/MEM is on the list for future inclusion.)



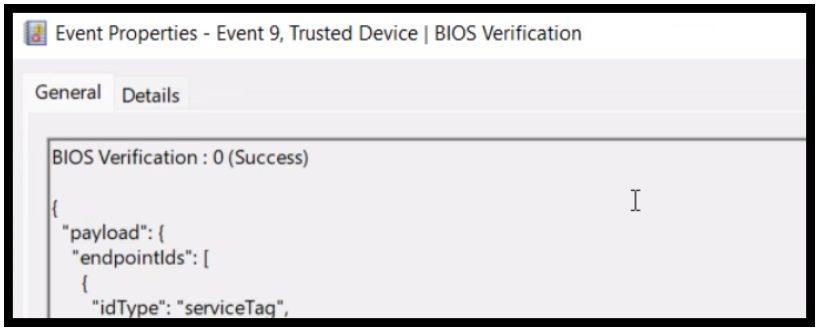
Security Score

This score provides a result denoting the endpoint's security level, based on different risk factors extracted from the hardware and operating system information. The result will be between 0 and 100, and risk areas scans show you why the device was scored to help the IT admin resolve any issues. The Indicators of Attack (IoA) information is mandatory for the overall success. This is also why this example has a score showing as "FAILED". The score will be generated after each start or, at most, over a 24-hour period.



BIOS verification

Microsoft Events also supports Command Line Interface for BIOS Verification.



SafeBIOS Indicators of Attack (IoA)

IoA provides results in two instances:

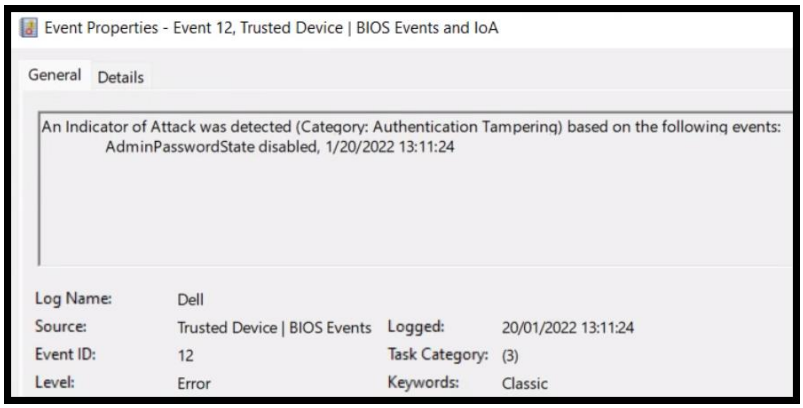
1) If any existing BIOS settings are not found to be compliant with recommended security practices, and

2) If changes are detected which indicate an attack is occurring, such as an unauthorized BIOS password change.

If you are using the default BIOS setting and still receive a failure notice, note that the default BIOS settings are usually generic and there is a need to check which settings make most sense for your situation and/or organization.

With Dell | Command Configure 4.4 software, Dell provides security settings which help to harden the BIOS further. You should understand however that if you are using these settings, they will impact solutions like the update of third-party apps and software in Windows Update. The UEFI encapsulated Firmware update is needed for Windows Update BIOS updates but it can be a risk to trust a UEFI update without other security in place, like a BIOS password. This is the reason why the security recommendation does not allow UEFI Firmware Update without a password.

Below is an example of an IoA security risk on a device with no Admin Password enabled. There could be a few other BIOS Events and IoA which shows other unsecured settings.



More information about Dell recommended BIOS settings can be found here:

[Dell Command | Configure Version 4.x Command Line Interface Reference Guide | Dell US]