

How to use Dell SafeBIOS in a modern management strategy

By Sven Riebe, Dell MCSG Technical Architect team

Edited by

Gus Chavira, Dell MCSG Technical Architect team and

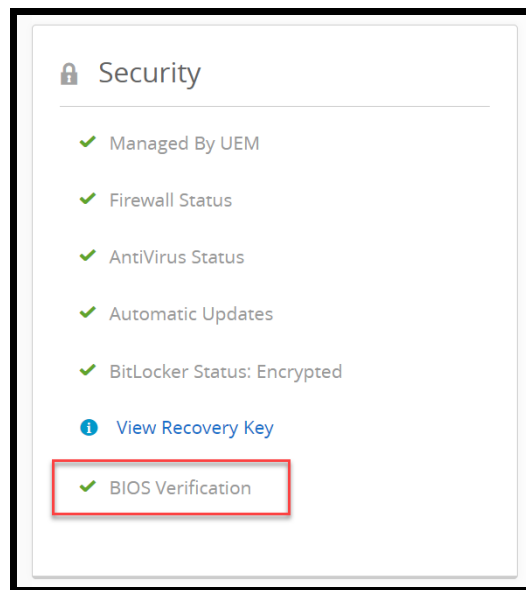
Amy Price, Dell MCSG Evangelist

Now that we understand what SafeBIOS is, how it works and what capabilities it brings to Dell endpoints, now we'll address some of the ways in which SafeBIOS has been integrated into the flow of client management tools.

Today's employees are working less frequently from inside the company network, spending their workdays at remote sites or working from a home office. With this increase in mobility, how is it possible to track the security status of their endpoints using corporate resources? The answer is to use cloud-based management for devices or security tools, like Microsoft Intune, VMware Workspace One and Carbon Black. In this section we will cover how to collect data from SafeBIOS using Workspace One UEM and the automation of this process based on the SafeBIOS results using Workspace One Intelligence.

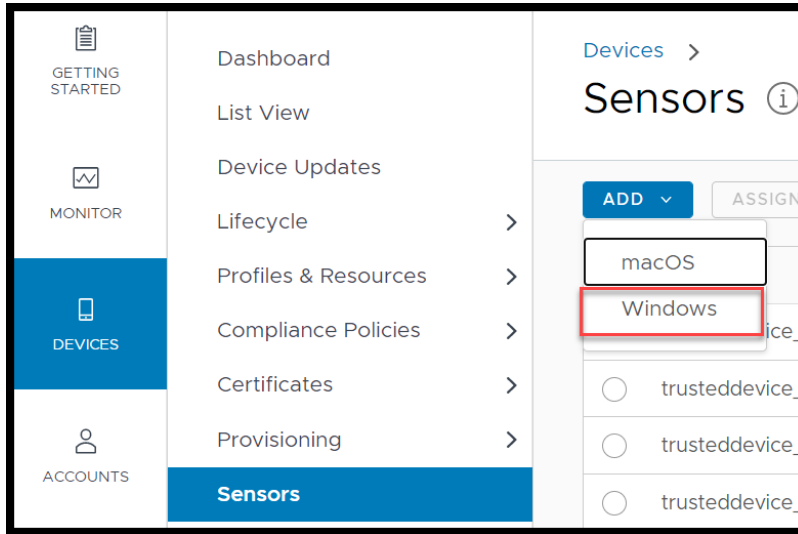
Dell SafeBIOS and Workspace One: Working Together

Dell and VMware have full integrations which combine Dell's client tools with VMware Workspace One, with Dell SafeBIOS being one example. Dell devices managed by Workspace One UEM with SafeBIOS report their BIOS verification status to the management console. Previously we have shown you above a couple of features of SafeBIOS but note that Workspace One UEM (formally AirWatch) is supporting BIOS verification only directly in the Workspace One UEM UI (User Interface).

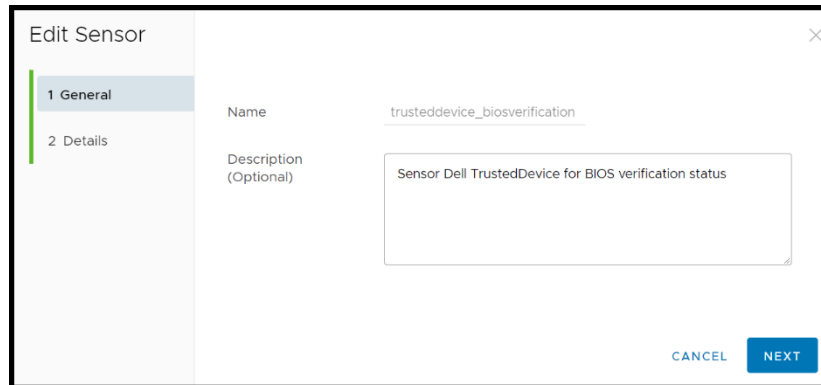


All other SafeBIOS features like Score and IoA are not shown directly in Workspace One UEM, but we can still extract this information using Workspace One Intelligence and Sensors and automate remediation workflows based on the results of SafeBIOS.

Workspace One UEM supports sensors. A sensor is a script which is run on a device and reports results back to Workspace One Intelligence. Workspace One supports sensors for Windows and MacOS. Here we will show examples of a couple of different sensors which allows collection from the full security data available from SafeBIOS that can then be used in Workspace One Intelligence.



You must supply a name for the sensor. This name you will find/use later in Workspace One Intelligence to use the data generated by the sensor.



In this example we are using a PowerShell script in the system context to generate requested data on the devices. Example sensors are located at this [GitHub repository](#).

[SvenRiebe/SafeBIOS \(github.com\)](https://github.com/SvenRiebe/SafeBIOS)

Please feel free to download for your own use and at your own risk with no warranties implied.

Edit Sensor

- 1 General
- 2 Details

Language: PowerShell

Execution Context: System

Execution Architecture: Auto

Response Data Type: String

Code UPLOAD ⓘ

```

12
13 Function DellTrustedDevice_SecurityAssessment() {
14     $ProviderName = "Trusted Device | Security Assessment"
15     $LogName = "Dell" # %SystemRoot%\System32\Winevt\Logs\Dell.evtx
16
17     $Result = Get-WinEvent -ProviderName $ProviderName -MaxEvents 1 # | format-
18     # Write-Host "`r\nTime: $($Result.TimeCreated)" -NoNewline

```

New Assignment

- 1 Definition
- 2 Deployment

Assignment Name: All Dell Devices

Select Smart Group: Start typing to add a group

Sensor All Devices (w/o VMs) [X]

CANCEL NEXT

New Assignment

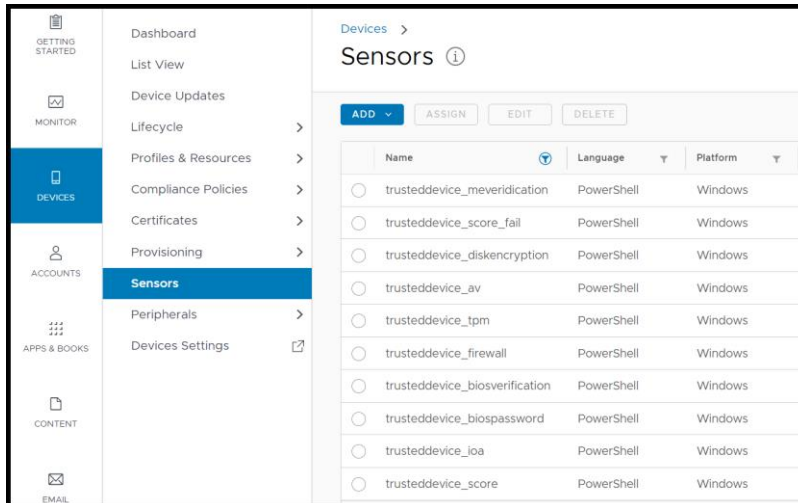
- 1 Definition
- 2 Deployment

Select which triggers should cause this sensor to run on assigned devices

Trigger Type: Event

- Login
- Log Out
- Startup
- User Switch

CANCEL BACK SAVE

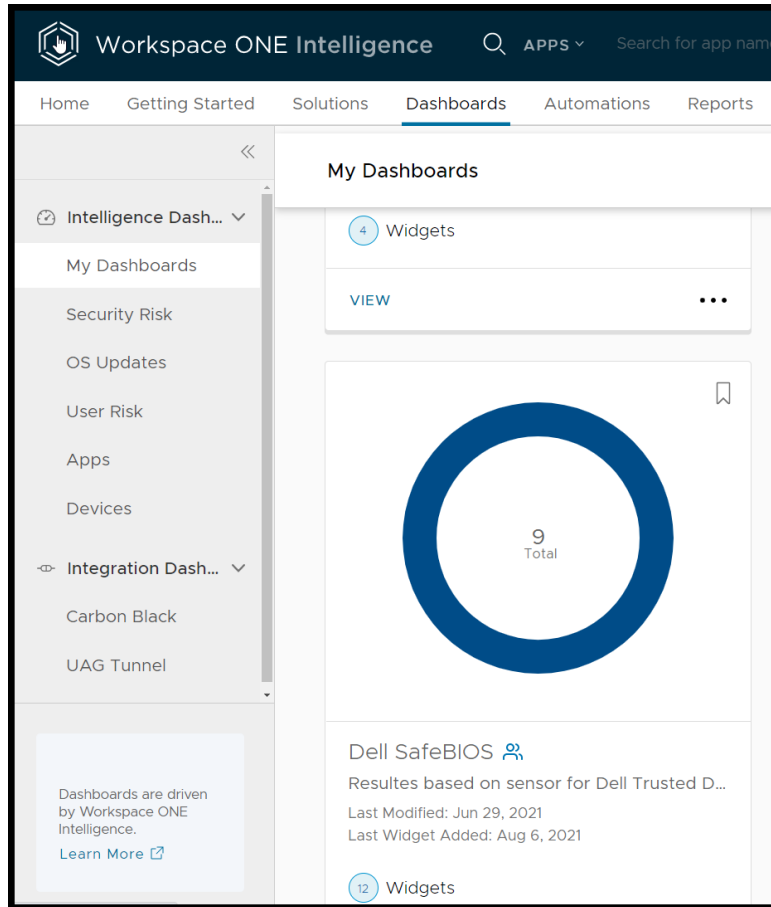


How you can use these sensors with Workspace One Intelligence

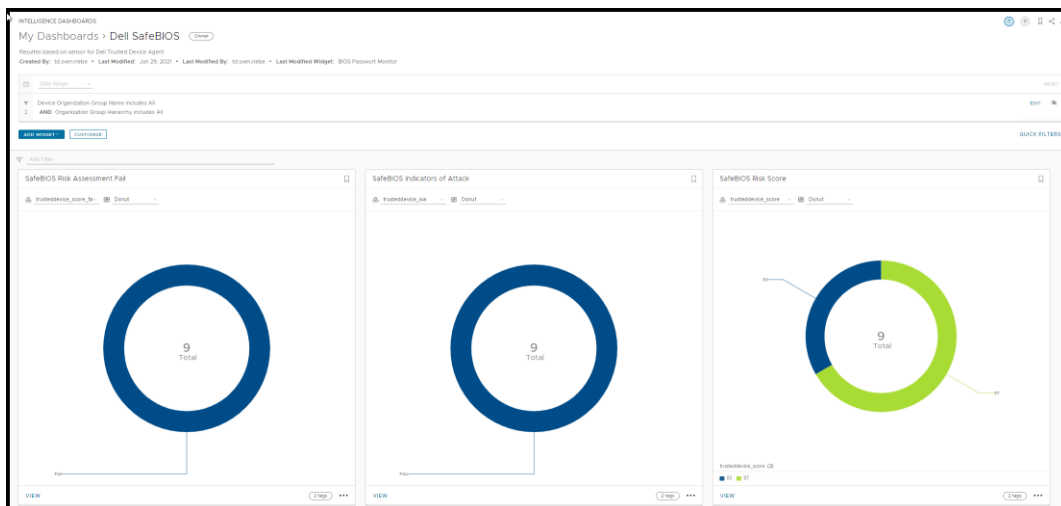
We will show you in this section how to build a SafeBIOS themed Dashboard along with automation to help with the security posture of an endpoint using Workspace One Intelligence and help your security IT Team get detailed information about the Device security from Dell SafeBIOS info.

We first need to create a Dashboard. Workspace One Intelligence Administrators can make their own dashboards and widgets using the results from Sensors to make these results visible.

In this case we have created a Dashboard that is collecting all SafeBIOS Sensor info to provide a view about score, risk and security status.



You could use different data pools to generate your own Dashboard. For my example I am using my generated sensors only.



If you want to make your own view you can add a Widget to the Dashboard, you have two options; the first option is you can use a template, or a second option is you make your own Widget like I have done.

You are free to choose output style like, Donut, Table, etc.

When devices have provided the first data, you can use your sensor and select the value for your Widget. You have the flexibility to build groups and subgroups. For my Indicators of Attack, I have grouped with the sensor only, but you can combine this with other sensors or UEM device data. You could also use filters e.g., to filter senseless values or unusual information.



Automation is the key in modernization

We now have a couple of pieces of information, but I don't want to check this each time, however for my risk management I need to investigate security related-issues soon as possible.

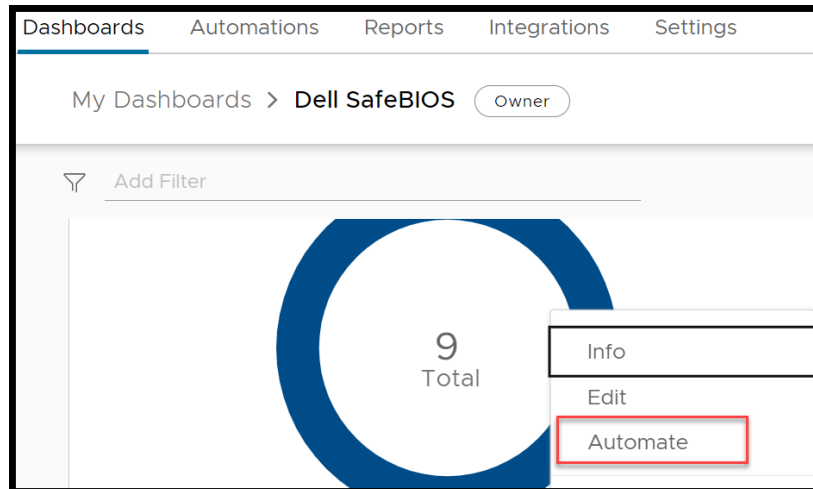
I made an example for you, showing how you could make an automatization based on sensors.

You could go to automate or choose this option direct in the sensor Dashboard. You will guide to generate a process like *send an e-mail*, or starting processes in ServiceNow. Workspace One UEM however is using Rest-API. In my case, if Indicators of Attack is showing a risk, Workspace One UEM should run an App which made BIOS settings to solve this problem.

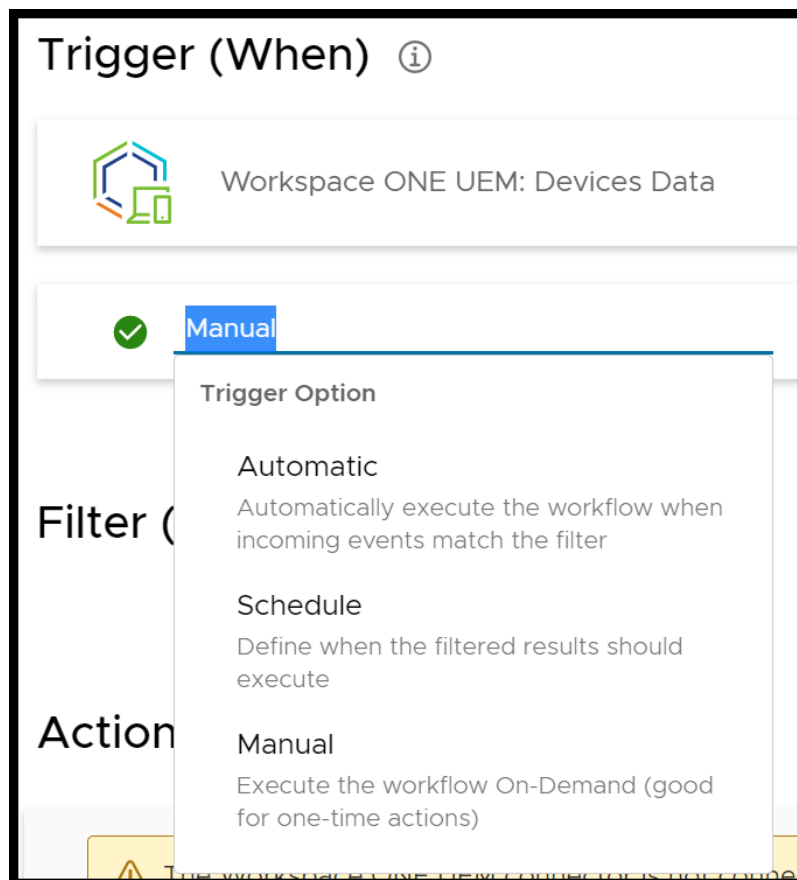
Option 1 over Automation



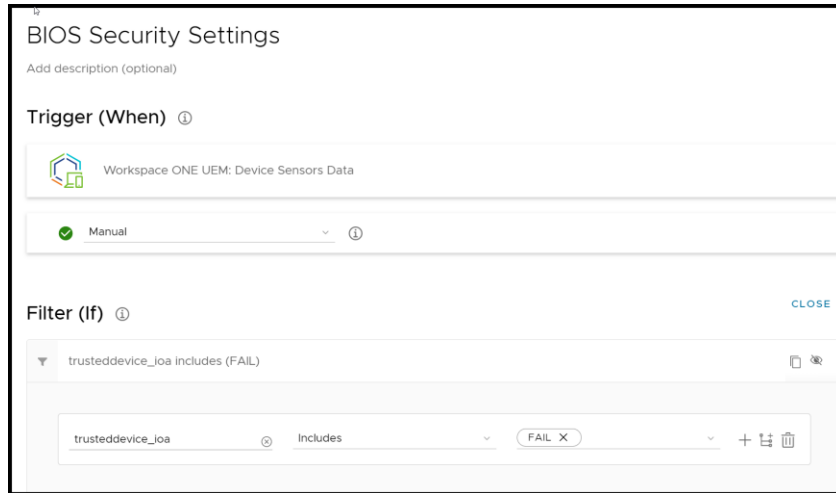
Option 2 direct from your dashboard.



If you are using the dashboard option, the filter will be the dashboard trigger - in my case the sensor indicators of attack. The automation needs a name e.g., BIOS Security Settings and you can choose if you want the automation full automatically, or manual and chosen by yourself.

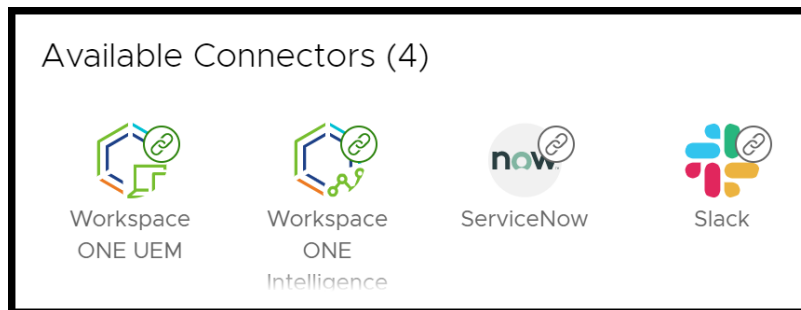


The workflow now has a name and a filter to identify the right devices which are needed for this workflow. In my scenario all devices will be selected which are failing for the IoA check.

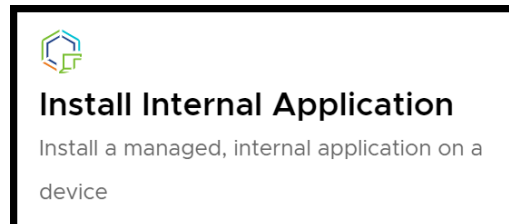


Workspace One Intelligence supporting REST-API. In my environment I have ServiceNow, Slack and Workspace One UEM/Intelligence.

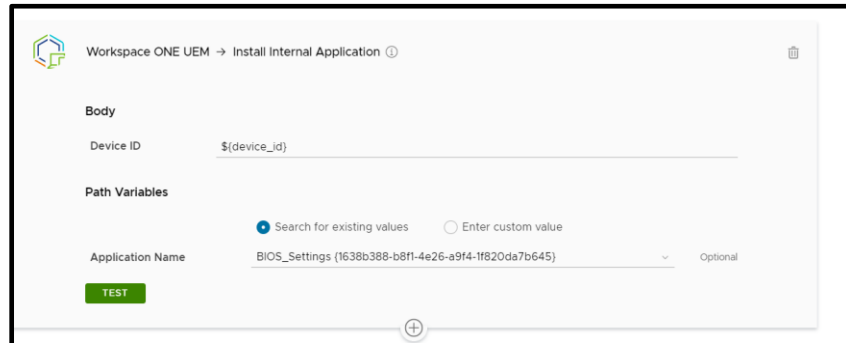
In my workflow I want to push new BIOS settings to all machines where the IoA check has failed. I will do this by Workspace One UEM where my App repository is available.



We have different options now like install a profile, delete device, etc. we are choosing Install Internal Application.

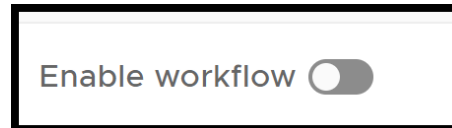


The device ID is managed by the workflow required to select the application. I have uploaded a PowerShell Script which makes the BIOS setting with the support of Dell Command Monitor which is installed on all my devices.

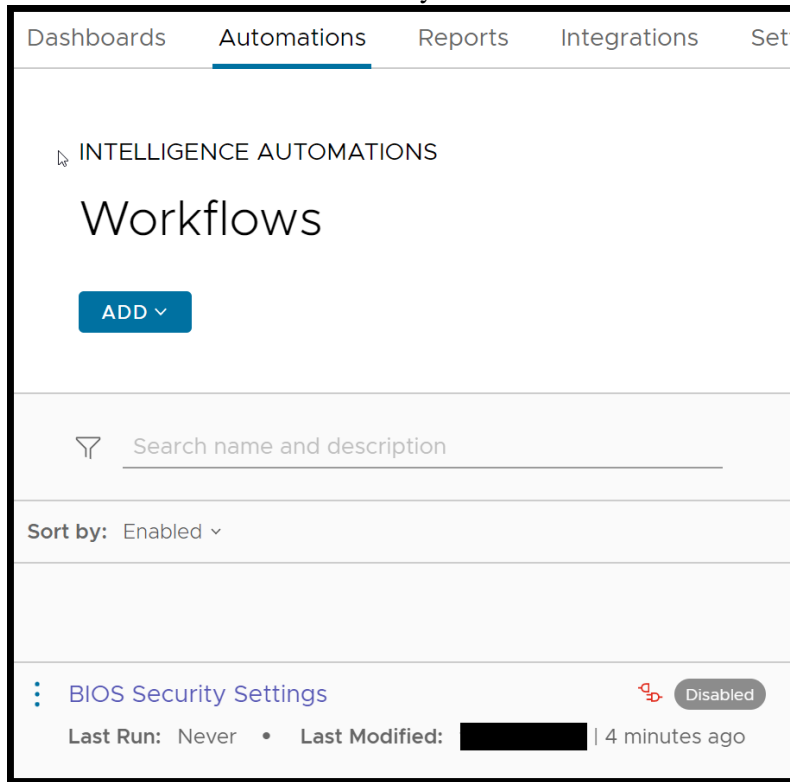


The screenshot shows the 'Install Internal Application' configuration page in Workspace ONE UEM. The page is titled 'Workspace ONE UEM → Install Internal Application'. It features a 'Body' section with a 'Device ID' field containing the PowerShell variable '\$(device_id)'. Below this is a 'Path Variables' section with two radio buttons: 'Search for existing values' (selected) and 'Enter custom value'. Underneath, there is an 'Application Name' dropdown menu with the selected value 'BIOS_Settings (1638b388-b8f1-4e26-a9f4-1f820da7b645)' and an 'Optional' label. A green 'TEST' button is located at the bottom left of the configuration area.

If you have selected the application and tested the workflow you can enable and disable the workflow. The automatic setting is the workflow is disabled, so you need to decide whether you want to workflow to run automatically.



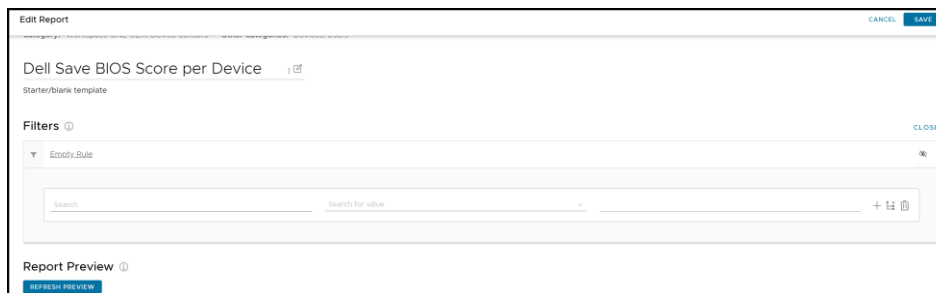
You can add/delete and edit your workflow as needed.



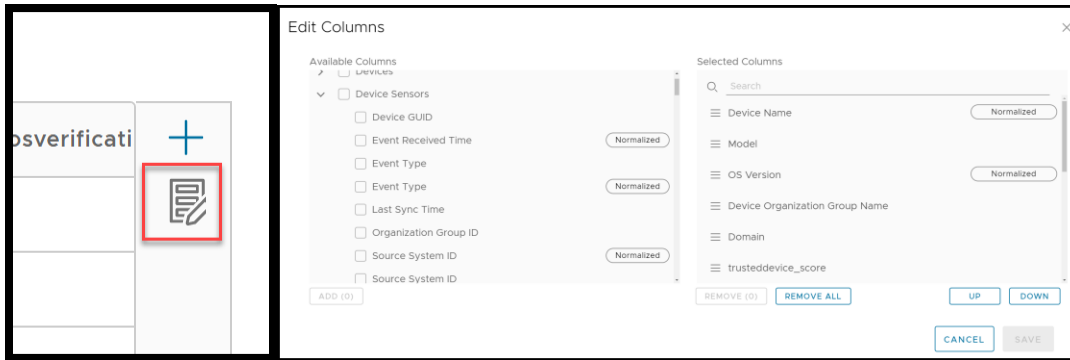
Generate Security Report.

If you have security administrators or CSOs in your company it could make sense to supply a security report on a scheduled basis. In Report it is quite simple to combine different values to get a useful report. For my project I want to generate a report of all SafeBIOS Sensors and send this report on weekly basis to my security team.

The report needs a name, and if you want to select a specific device to scan, then use the filter choice.



We can select all fields we need for our report. We have wide options of Workspace One fields, sensors, etc.



If we are finished, we can save the report, and now we can share or automate this report for our needs.

Dashboards Automations **Reports** Integrations Settings

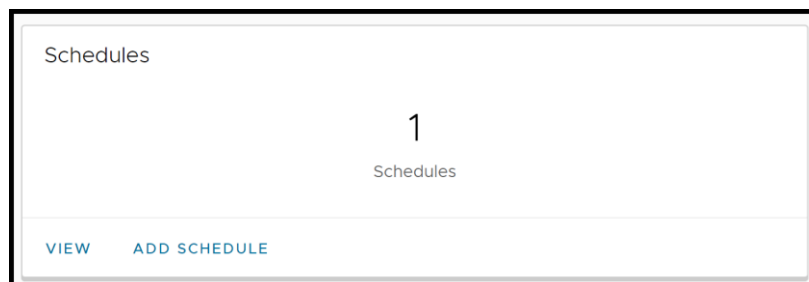
Reports > Dell Save BIOS Score per Device Owner: Overview

Empty Rule

Preview ¹
This report has 9 records. Refreshed a few seconds ago

Device Name	Model	OS Version	Device Organization Group Na...	Domain	trusteddevice_sco...	Last Seen	trusteddevice_...	trusteddev...
itpro-6	Latitude 7300	10.0.19042			87	Sep 27, 2021 11:04 A...	PASS	PASS
itpro-6	Latitude 7400 2-in-1	10.0.19042			87	Oct 20, 2021 4:21 PM	PASS	PASS
itpro-7	Latitude 7320 Detacha...	10.0.19043			87	Feb 1, 2022 1:47 PM	PASS	WARNING
itpro-5	Latitude 5300	10.0.19042			83	Sep 29, 2021 2:51 PM	PASS	WARNING
itpro-3	Precision 5750	10.0.19043			87	Feb 1, 2022 9:36 AM	PASS	PASS
itpro-3	Latitude 7310	10.0.19042			87	Sep 27, 2021 11:00 A...	PASS	PASS
itpro-1	Latitude 9510	10.0.19043			83	Jan 11, 2022 2:50 PM	PASS	PASS

It does not make sense to check this report manually in a large company, so I am making a schedule of this report which I want to provide to my security team.



We have a couple of options for report scheduling. I am configuring the report on weekly basis at 12pm. I am now getting an email each Monday with a link to my new report. The reports will also be stored so I will have a history of my reports in the future.

Schedule: Dell Save BIOS Score per Device ✕

Schedule Name: Dell Trusted Device Report for Security Team

Recurrence: Weekly

Day(s) of the week: M T W T F S S

Starts At: 12:00 CET ⓘ

Ends: NO END DATE END BY

CANCEL
SCHEDULE

Carbon Black integration

VMware security products have a full integration of Dell Safe BIOS, so it is very simple to use this feature. Dell Device with SafeBios can be also be monitored by Carbon Black. The chapter Live Query provides a standard Query to check the status of Dell Safe BIOS, which allows Carbon Black Administrators to take actions based on the results. An example could be to disconnect device if the BIOS is looking affected by an attack to secure the Company environment.

The screenshot shows the Carbon Black Cloud interface. On the left is a navigation sidebar with options like Dashboard, Alerts, Investigate, Live Query, Enforce, Harden, Inventory, and Settings. The main area is titled 'NEW QUERY' and shows a 'Recommended' tab with several query categories: All (95), IT Hygiene (26), Vulnerability Mgmt (17), Threat Hunting (30), and Compliance (22). The 'IT Hygiene' category is selected. Below this, there's a search bar and a dropdown for 'OS'. A description box for the selected query reads: 'Description: On Windows XP and later operating systems, credential theft tools (such as Mimikatz) can access the WDigest protocol that sends plain text credentials to certain applications. By default, Windows stores these credentials in the lsass.exe process for user convenience. This protocol should be disabled. Learn more: https://attack.mitre.org/techniques/T1003/'. The results section shows: 'Results: Lists 0 for all systems that have UseLogonCredential disabled. If no results are returned, CB recommends deploying this IT Hygiene policy via GPO to protect against credential theft. If results are 1 for Windows 10 or Windows 2016, CB recommends conducting an immediate investigation. Carbon Black recommends that you run this query daily'. At the bottom, the query name 'Dell SafeBIOS Verification Status' is shown with 'Schedule' and 'Run' buttons. A SQL query is visible at the bottom: 'WITH b1 AS (SELECT COUNT(*) AS cnt, 1 AS one FROM #table)'. There are also 'Edit SQL' and 'Collapse' options.

After running the query, the Carbon Black Agent on the local machines reports the device Safe BIOS status to the Carbon Black Console.

If you have Workspace One Intelligence in place you can use the Carbon Black integration. This integration gives you the same availabilities as I am using above in my Workspace One scenario.

