Custom Compliance and Remediation with Microsoft Endpoint Manager (Intune)

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.

If we are talking about Modern Management, we don´t want forget MS Intune. MS Intune has supported some new features since December 2021, but please check first if your MS License includes these features, if not you will have to pay additional to Microsoft for this service.

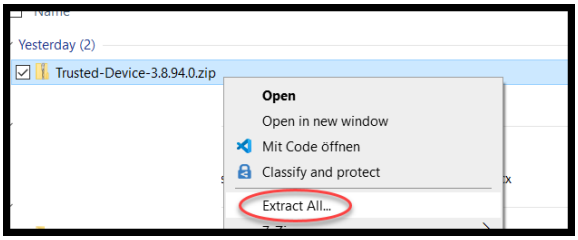
Before we start with the Compliance, we need install the Safe BIOS Agent on the device. We will show how it works with Microsoft Intune.

Prepare Dell Trusted Device Agent for MEM (Microsoft Endpoint Manager)

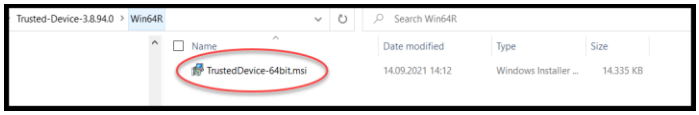
Download of the newest Version of Dell Trusted Device Agent from the Dell website.

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

The file must be unzipped:

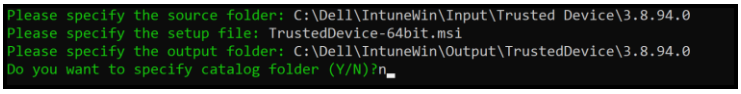


The folder contains a file named TrustedDevice-64bit.msi. This file is required for deploying the software package through MEM.

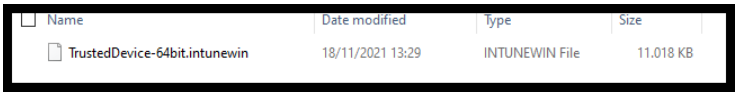


Start the Microsoft Win32 Content Prep Tool (aka MEMAppUtil.exe). In case you are not familiar with this tool, you will find documentation here: https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-prepare

Argument	Value
Source Folder	folder where you have stored the unzipped MSI
Setup file	Main installer file like msi/exe/ps1, etc.
Output Folder	where you want to store the IntuneWin



MEM is now prepared and ready for installation by MEM.



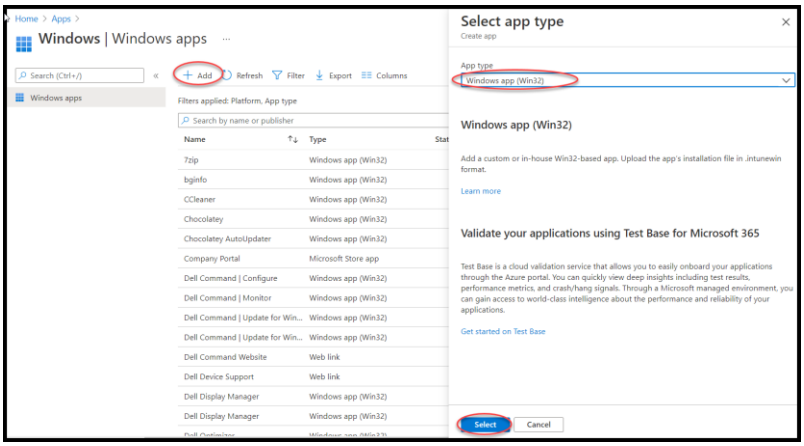
Import and Deployment settings Dell Trusted Device Agent for MEM

Click ‘Add’

Field	Value
Source Folder	Windows app (Win32)

Click ‘Select’

Select Windows app (Win32) as application.



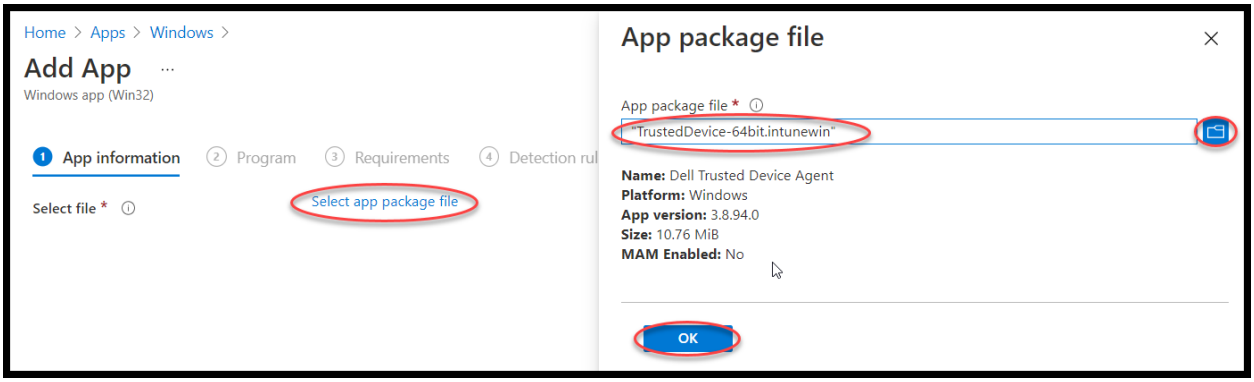
Section ‘App information’

Click ‘Select app package file’

Click ‘Folder’

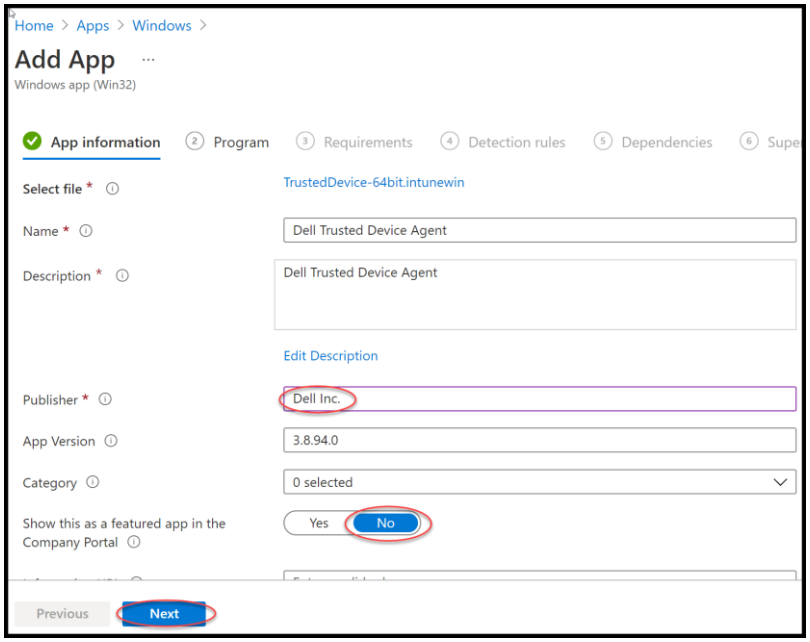
Select ‘TrustedDevice-64bit.intunewin’

Click ‘OK’



Field	Value
Publisher	Dell Inc.
Show this as a featured app in the Company Portal	No (default security app by device)

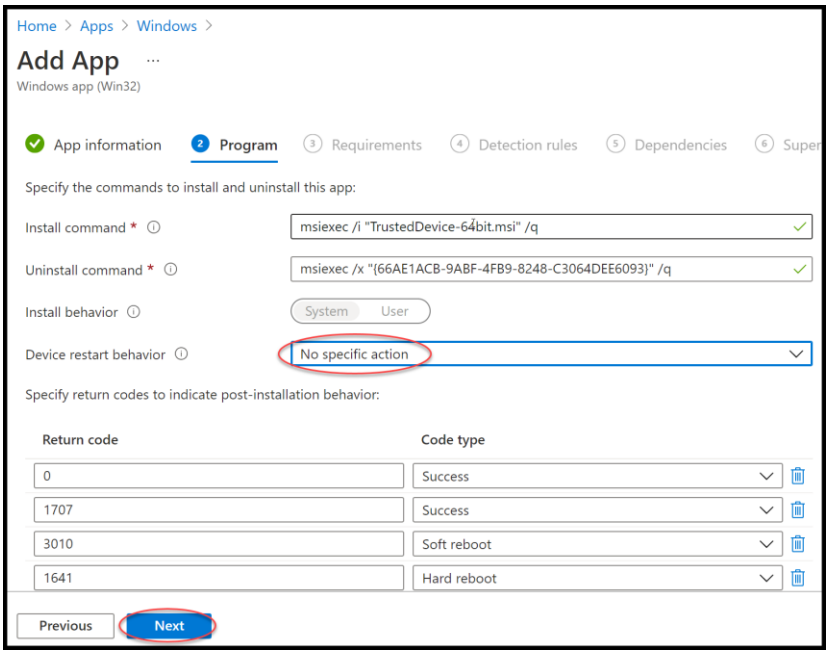
Click 'Next'



Section ‘Program’

Field	Value
Device restart behavior	No specific action

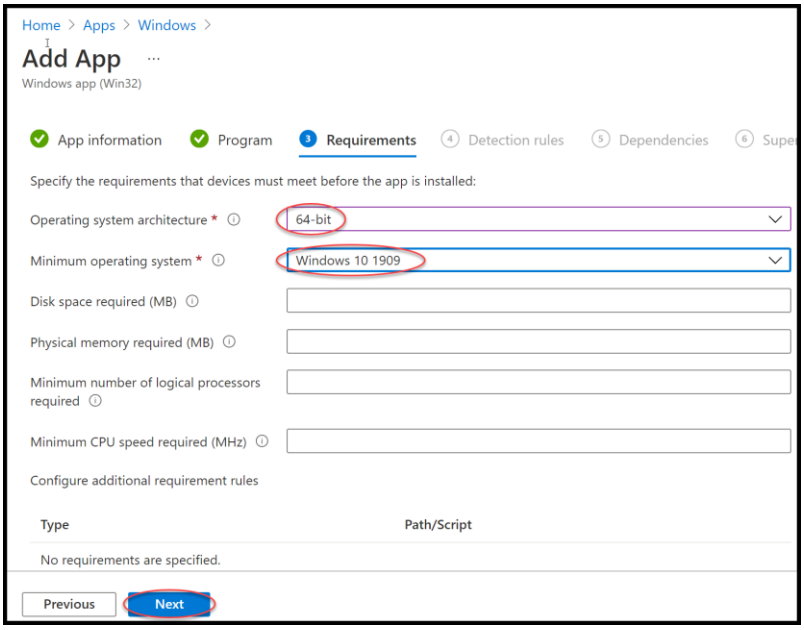
Click ‘Next’



Section ‘Requirements’

Field	Value
Operating system architecture	64-Bit
Minimum operating system	1909 (Please note Dell support drivers and software only with the latest Win version + N -2)

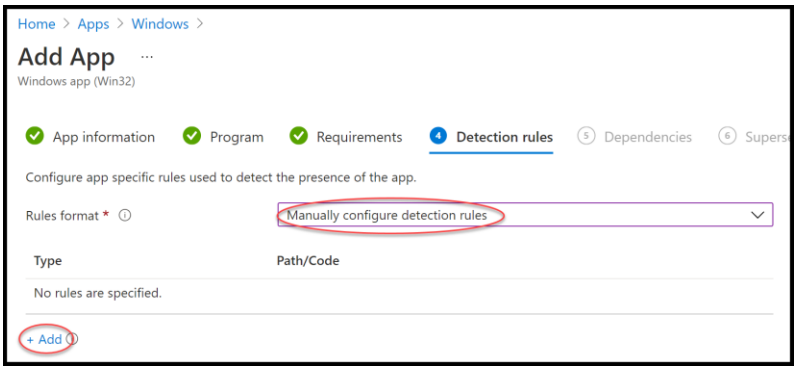
Click ‘Next’



Section ‘Detection rules’

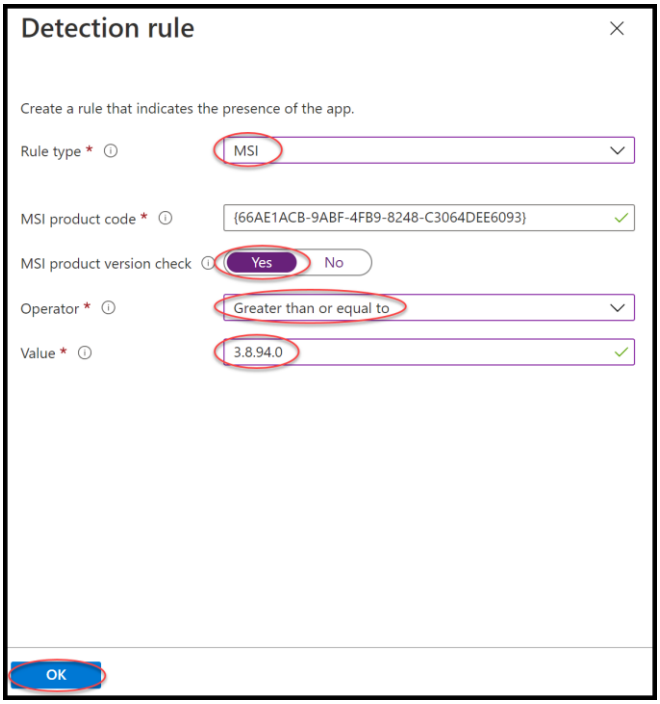
Field	Value
Rules format	Manually configure detection rules

Click ‘Add’

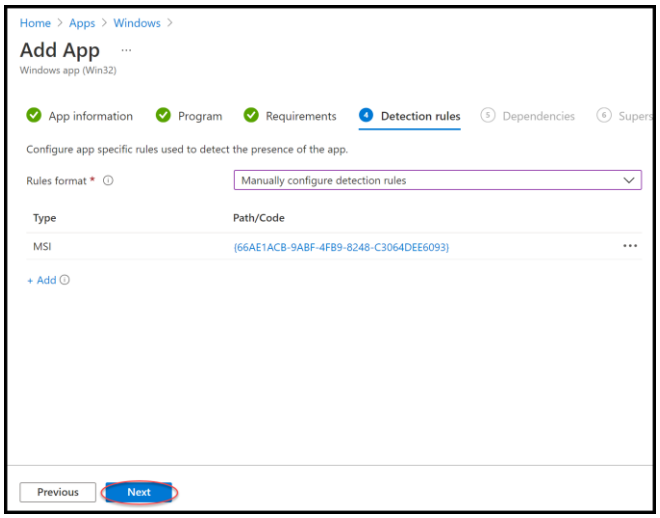


Field	Value
Rule type	MSI
MSI product code	Default
MSI product version check	Yes
Operator	Greater than or equal to
Value	3.8.94.0 **Note:** Use version of your Trusted Device

Click ‘OK’



Click ‘Next’


Home > Apps > Windows >
Add App
Windows app (Win32)
App information
Program
Requirements
4 Detection rules
Dependencies
Configure app specific rules used to detect the presence of the app.
Rules format *
Manually configure detection rules
Type
Path/Code
MSI
{66AE1ACB-9ABF-4FB9-8248-C3064DEE6093}
+ Add
Previous
Next

Section ‘Dependencies’

No changes

Section ‘Supersedence’

No changes

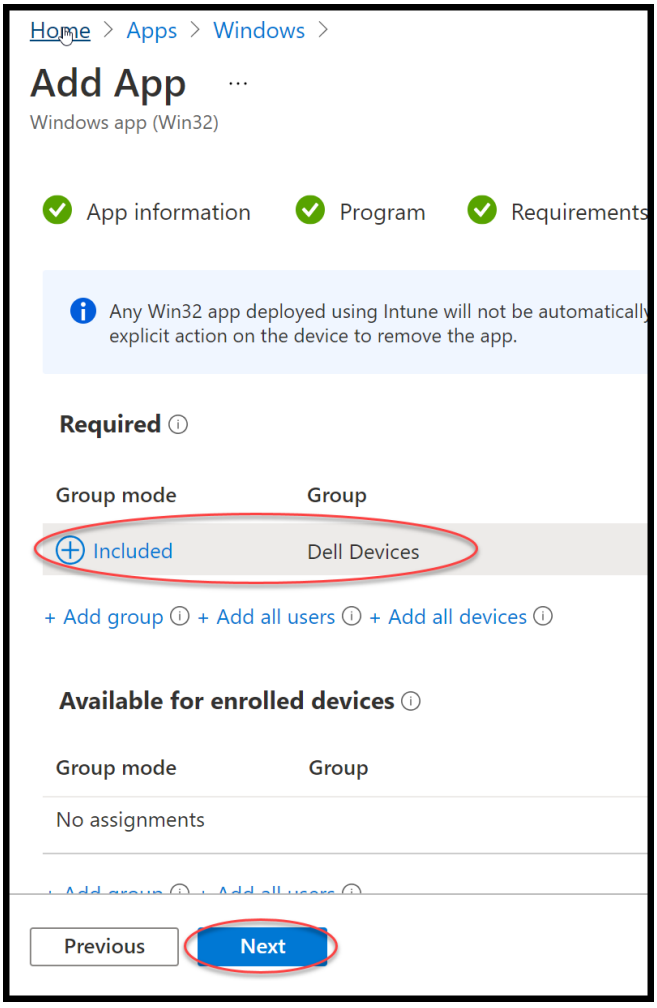
Note: If you have an existing version of this software, you can select the previous version at this stage to uninstall before this soft package is installed. All install instructions are tested for Install/Uninstall and Update, so to uninstall the old one is not necessary.

Section ‘Assignments’

The Dell Trusted Device Agent supports only Dell (Latitude, Optiplex, Precision and mobile XPS) it makes sense to have a dynamic group which only incl. these systems.

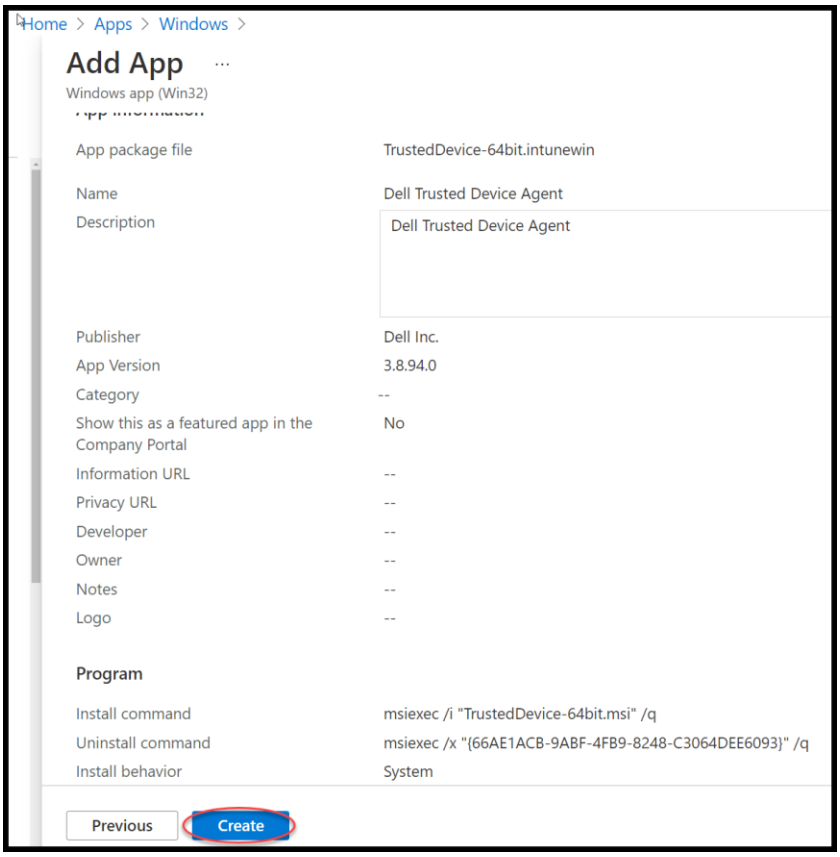
Option	Value
Required	Add group ‘Dell Devices’
Available for enrolled devices	
Uninstall	

Click ‘Next’



The app is now finished

Click ‘Create’



Ready to work.

Custom Compliance Reporting

MS Intune now supports custom compliance reporting, which allows you to make your own compliance policies if you want. This feature needs a JSON file to manage the reporting and a PowerShell script to collect the data from the managed devices.

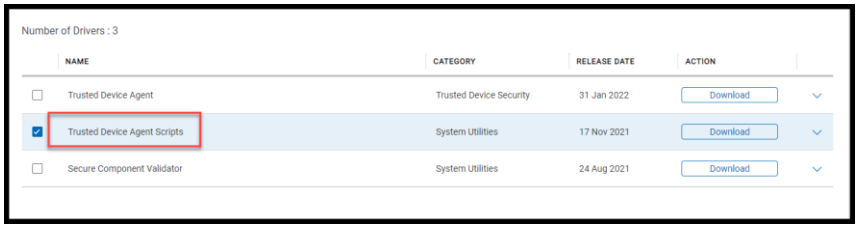
You will find the Microsoft documentation here: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-use-custom-settings

My JSON file and the PowerShell script you will find here:

https://github.com/svenriebedell/Intune

The official Dell files you will find here:

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



JSON file:

```
{
  "Rules":[
    {
      "SettingName":"SecurityScore",
      "Operator":"GreaterThan",
      "DataType":"Int64",
      "Operand":"80",
      "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
      "RemediationStrings":[
        {
          "Language":"en_US",
          "Title":"Security Score is {ActualValue} please check for reasons.",
          "Description": "Investigation for security is needed"
        }
      ]
    },
    {
      "SettingName":"TPM",
      "Operator":"IsEquals",
      "DataType":"String",
      "Operand":"PASS",
      "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
      "RemediationStrings":[
        {
          "Language": "en_US",
          "Title": "TPM chip must be enabled.",
          "Description": "TPM chip must be enabled. Please refer to the link above"
        }
      ]
    },
    {
      "SettingName":"BIOSVerfication",
      "Operator":"IsEquals",
      "DataType":"String",
      "Operand":"PASS",
```

```
        "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "Trusted Device not installed or supported.",
            "Description": "Dell Trusted Device Agent save the BIOS."
          }
        ]
      },
      {
        "SettingName":"DiskEncryption",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"PASS",
        "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "Disk Encryption is not enabled for the Device.",
            "Description": "Go to Microsoft Security Center enable Bitlocker or other solution."
          }
        ]
      },
      {
        "SettingName":"Firewall",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"PASS",
        "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "Firewall is not enabled for the Device.",
            "Description": "Go to Microsoft Security Center enable MS Firewall/Defender or other solution."
          }
        ]
      },
      {
        "SettingName":"AntiVirus",
        "Operator":"IsEquals",
        "DataType":"String",
```

```
        "Operand":"PASS",
        "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
        "RemediationStrings":[
            {
              "Language": "en_US",
              "Title": "AntiVirus is not enabled for the Device.",
              "Description": "Go to Microsoft Security Center enable MS Defender or other solution."
            }
          ]
        },
        {
        "SettingName":"BIOSAdminPW",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"PASS",
        "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
        "RemediationStrings":[
            {
              "Language": "en_US",
              "Title": "No BIOS Password is set on the machine.",
              "Description": "Asking your administrator to enable a password."
            }
          ]
        },
        {
        "SettingName":"vProVerification",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"PASS",
        "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
        "RemediationStrings":[
            {
              "Language": "en_US",
              "Title": "vPro Management is effect.",
              "Description": "Please contact your administator in behalf of a security issue."
            }
          ]
        },
        {
        "SettingName":"IndicatorOfAttack",
        "Operator":"IsEquals",
        "DataType":"String",
```

```
        "Operand":"PASS",
        "MoreInfoUrl":"https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device",
        "RemediationStrings":[
            {
              "Language": "en_US",
              "Title": "BIOS settings need to be check.",
              "Description": "Please contact your administrator on behalf of a security issue."
            }
          ]
      }
   ]
  }
```

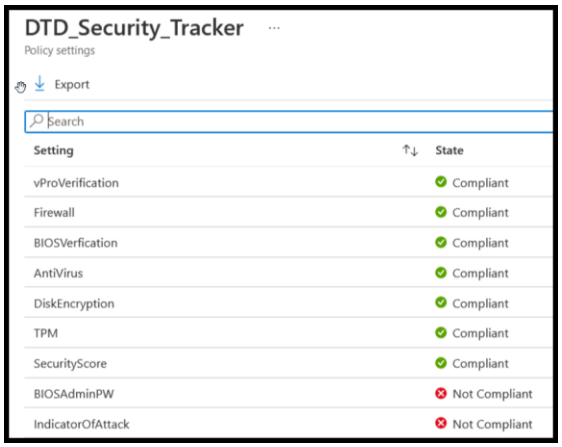
PowerShell script

```
<#
_author_ = Sven Riebe <sven_riebe@Dell.com>
_twitter_ = @SvenRiebe
_version_ = 1.0.1
_Dev_Status_ = Test
Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved.

No implied support and test in test environment/device before using in any production environment.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at
   http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
#>

<#Version Changes

1.0.0   inital version
1.0.1   integrated function for selection values and rework String Cut by select last Word


#>

<#
.Synopsis
   This PowerShell is for custom compliance scans and is checking Microsoft event for the Dell security score provide by Trusted Device Agent
```

```
  IMPORTANT: This script need a client installation of Dell Trusted Device Agent.
https://www.dell.com/support/home/en-us/product-support/product/trusted-device/drivers
  IMPORTANT: This script does not reboot the system to apply or query system.
.DESCRIPTION
  PowerShell using Microsoft event log to check the Security Score and option compliances of Dell
Trusted Device Agent. This script needs to be upload in Intune Compliance / Script and need a JSON file
additional for reporting this value.

#>


# Function for snipping SafeBIOS values from the MS Event
function Get-SafeBIOSValue{

   # Parameter
   param(
      [string]$Value

       )

   # Collect last MS Event for Trusted Device | Security Assessment
   $SelectLastLog = Get-EventLog -LogName Dell -Source "Trusted Device | Security Assessment" -
Newest 1 | select -ExpandProperty message

   # Prepare value for single line and value

   $ScoreValue = ($SelectLastLog.Split([Environment]::newline) | Select-String $Value)
   $ScoreLine = ($ScoreValue.Line).Split(' ')[-1]

   $ScoreValue = $ScoreLine

   Return $ScoreValue

}

#Select score values
$OutputScore = Get-SafeBIOSValue -Value 'Score'
$OutputAntivirus = Get-SafeBIOSValue -Value 'Antivirus'
$OutputAdminPW = Get-SafeBIOSValue -Value 'BIOS Admin'
$OutputBIOSVerify = Get-SafeBIOSValue -Value 'BIOS Verification'
$OutputMEVerify = Get-SafeBIOSValue -Value 'ME Verification'
$OutputDiskEncrypt = Get-SafeBIOSValue -Value 'Disk Encryption'
$OutputFirewall = Get-SafeBIOSValue -Value 'Firewall solution'
$OutputIOA = Get-SafeBIOSValue -Value 'Indicators of Attack'
$OutputTPM = Get-SafeBIOSValue -Value 'TPM enabled'



# Devices without vPro should be pass the later compliance process as well but Intune could be handle
only Pass or Fail, all devices without vPro Pass this section
if ($OutputMEVerify -match 'UNAVAILABLE')
```

```
    {
    $OutputMEVerify = 'Pass'
    }
Else
    {
    #No action needed
    }

#prepare variable for Intune
$hash = @{ SecurityScore = $OutputScore; AntiVirus = $OutputAntivirus; BIOSAdminPW =
$OutputAdminPW; BIOSVerfication = $OutputBIOSVerify; DiskEncryption =
$OutputDiskEncrypt;Firewall = $OutputFirewall; IndicatorOfAttack = $OutputIOA; TPM =
$OutputTPM; vProVerification = $OutputMEVerify}

#convert variable to JSON format
return $hash | ConvertTo-Json -Compress
```

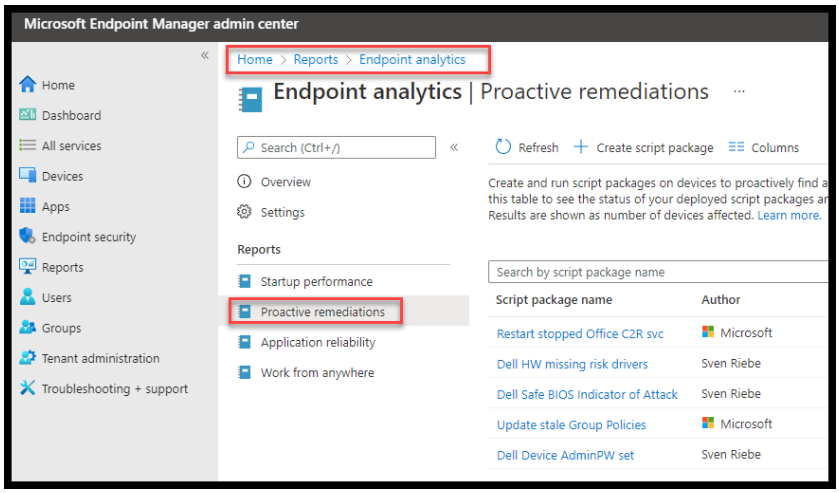
If you have prepared and assigned your custom compliance it could look like this.



MS Intune offers customers with E3 or E5 license contracts a new feature, Proactive Remediations, which allows you to check specific values from a managed device and then starting actions if the detection finds any issues.

You find the Microsoft documentation here: https://docs.microsoft.com/en-us/mem/analytics/proactive-remediations

You will find this feature in the ‘Report’ section.



As an example I will check in the Safe BIOS Security Score devices a failed Indicator of Attack. We need two PowerShell scripts; Detection and Remediation.

Script for detection:

```
<#
_author_ = Sven Riebe <sven_riebe@Dell.com>
_twitter_ = @SvenRiebe
_version_ = 1.0.1
_Dev_Status_ = Test
Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved.

No implied support and test in test environment/device before using in any production environment.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at
   http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
#>

<#Changes
1.0.0 initial Version
1.0.1 Change line 37 from InstanceID 15 to Source "Trusted Device | Security Assessment"
#>

<#
.Synopsis
   This PowerShell is checking Microsoft Event for the Dell Trusted Device Secure Score and then if the
IoA Indicators of attack is failing or not.
```

```
  IMPORTANT: Need to install Dell Trusted Device first Version 3.2 or newer
  IMPORTANT: This script does not reboot the system to apply or query system.
.DESCRIPTION
  PowerShell to import as detection Script for Microsoft Endpoint Manager. This Script need to be
imported in Reports/Endpoint Analytics/Proactive remediation. This File is for detection only and need a
separate script for remediation additional.

#>

try{
   # Check if Safe BIOS IOA is failed
   $SelectLastLog = Get-EventLog -LogName Dell -Source "Trusted Device | Security Assessment" -
Newest 1 | select -ExpandProperty message
   $SelectIOA = ($SelectLastLog.Split([Environment]::newline) | Select-String 'Indicators of Attack')
   $CheckIOA = ($SelectIOA.Line).Split(' ')

   if ($CheckIOA[5] -match "PASS")
      {
      write-host "Success"
          exit 0
      }
   Else
      {
      Write-Host "Missing BIOS Settings"
      exit 1
      }
   }
catch
{
   $errMsg = $_.Exception.Message
   write-host $errMsg
   exit 1
}
```

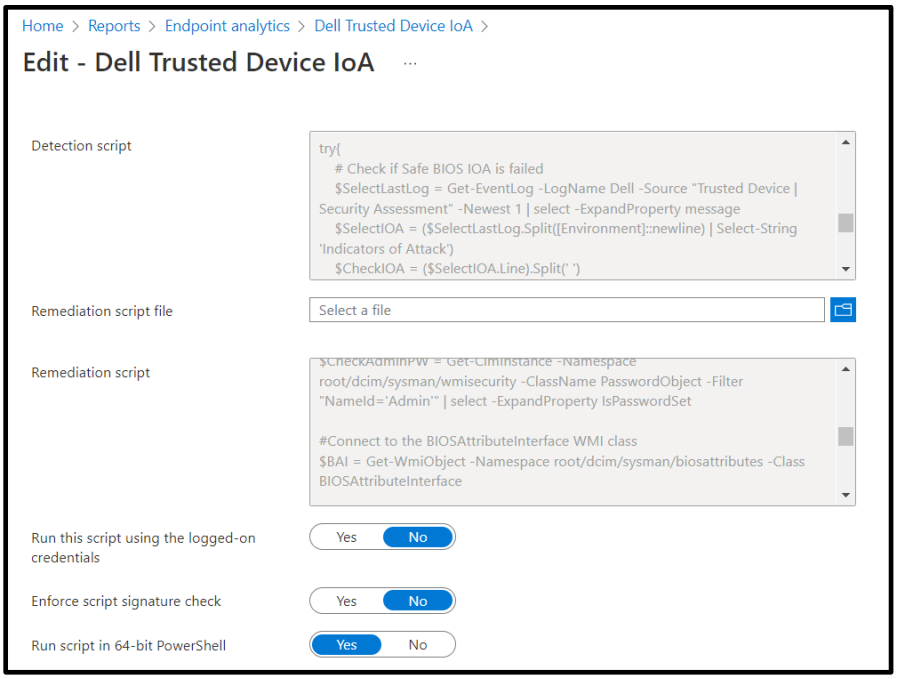
Script remediation:

```
<#
_author_ = Sven Riebe <sven_riebe@Dell.com>
_twitter_ = @SvenRiebe
_version_ = 1.0.0
_Dev_Status_ = Test
Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved.

No implied support and test in test environment/device before using in any production environment.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at
   http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
```

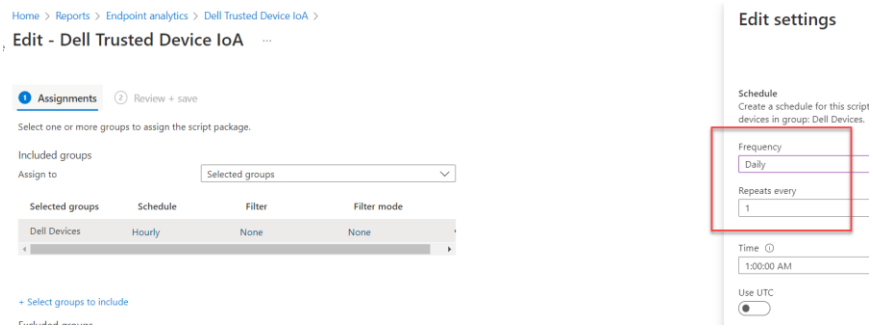
```
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
#>

<#Version Changes

1.0.0   inital version


#>

<#
.Synopsis
   This PowerShell is for remediation by MS Endpoint Manager. This script will set BIOS a couple of BIOS settings from default to IoA required settings
   IMPORTANT: WMI BIOS is supported only on devices which develop after 2018, older devices do not supported by this PowerShell
   IMPORTANT: This script does not reboot the system to apply or query system.  (Put in any reboot requirements if applicable here)
.DESCRIPTION
   PowerShell using WMI for setting couple of BIOS settings machine. The script checking if any PW is existing and handover the right credentials to WMI for BIOS setting or if AdminPW is not set it make a simple BIOS setting without credentials. This Script need to be imported in Reports/Endpoint Analytics/Proactive remediation. This File is for remediation only and need a separate script for detection additional.

#>


# Control check by WMI
$CheckAdminPW = Get-CimInstance -Namespace root/dcim/sysman/wmisecurity -ClassName PasswordObject -Filter "NameId='Admin'" | select -ExpandProperty IsPasswordSet

#Connect to the BIOSAttributeInterface WMI class
$BAI = Get-WmiObject -Namespace root/dcim/sysman/biosattributes -Class BIOSAttributeInterface

if ($CheckAdminPW -eq 0)
    {

    # set FastBoot Thorough by WMI
    $BAI.SetAttribute(0,0,0,"AllowBiosDowngrade","Disabled")
    $BAI.SetAttribute(0,0,0,"StrongPassword","Enabled")
    $BAI.SetAttribute(0,0,0,"CapsuleFirmwareUpdate","Disabled")
    $BAI.SetAttribute(0,0,0,"WakeOnDock","Disabled")

    Write-Output "BIOS settings without BIOS PW possible"

    Exit 0
    }
```

```
Else
   {

   # Select AdminPW for this device
   $AdminPw = "Your AdminPW Password”

   # Encoding BIOS Password
   $Encoder = New-Object System.Text.UTF8Encoding
   $Bytes = $Encoder.GetBytes($AdminPw)


   # set FastBoot Thorough by WMI with AdminPW authorization
   $BAI.SetAttribute(1,$Bytes.Length,$Bytes,"AllowBiosDowngrade","Disabled")
   $BAI.SetAttribute(1,$Bytes.Length,$Bytes,"StrongPassword","Enabled")
   $BAI.SetAttribute(1,$Bytes.Length,$Bytes,"CapsuleFirmwareUpdate","Disabled")
   $BAI.SetAttribute(1,$Bytes.Length,$Bytes,"WakeOnDock","Disabled")

   Write-Output "BIOS settings needs BIOS PW"

   Exit 0
   }
```

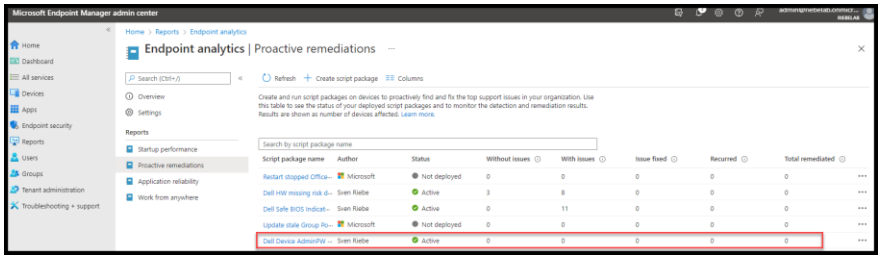
If I have uploaded both scripts and assigned this to a specific group of devices, it is ready to use. Please check the Microsoft manual for more details.



You can decide at the assignment how often the detection should be running. Once per hour should be matched to the checked value. In my example, the Safe BIOS Secure Score is running either at the start up of a device, or every 24 hours, because it doesn't make sense to run the detection every hour since the value doesn't change on an hourly basis.



Now you can monitor the detection and remediation for your devices.



Many thanks for reading this Blog. I hope it shows you how simple it is to attach more security to your environment. Let me know if you have any other ideas for workflows and detection.

Contact me by Linkedin: https://de.linkedin.com/in/svenriebe

Or by Twitter: @SvenRiebe

Or feel free to message me within the DTUWC platform