Notes From the Field

MDE Lessons Learned

Migrating from 3rd party AV

Rob Strawley, Sr. Cybersecurity Consultant

Microsoft

MDE Processes

- MsSense.exe- The actual MDE service that provides cyber telemetry and “wakes up” upon onboarding.
- SenseCnCProxy.exe- C2 channel for SenseIR service
- SenseIR.exe- The Magic of MDE, conducts the remediation instructions, Live Response, etc.
- Sense CE- Endpoint DLP Classification service
- SenseSampleUploader.exe- similar to MAPS only submits sample to MDE tenant for analysis.
- **SenseNDR**- Neighbor Discovery of “rogue” devices

MDAV on Windows 10

- By default goes into Disabled Mode as long as an up to date 3rd party AV is Active. Automatically goes into Active mode once 3rd party AV is removed
- Can run along side 3rd party AV in Passive Mode for EDR Block Mode
- Some vendor AV writes a registry to “hard disable”.
- Check for GPO’s that disable MDAV before Migration- remember, MDAV is disabled by default - it makes a difference!

MDE on Windows 10

- Manual Remediation Actions from MDE portal- started with Windows 10 1703
- MDE AIR- Windows 1809 (technically started with 1709 OS Build 16299.1085 with KB4493441)- recommend customers to minimum Windows 1809.

Endpoint protection on down-level Operation systems

- Windows XP- no support at all. Upgrade your systems. Period.
- Windows 7, 8.1:

-Must install System Center Endpoint Protection (SCEP)

-Must install Microsoft Monitoring Agent (MMA)

-MDE is an EDR only- no AIR features….yet.

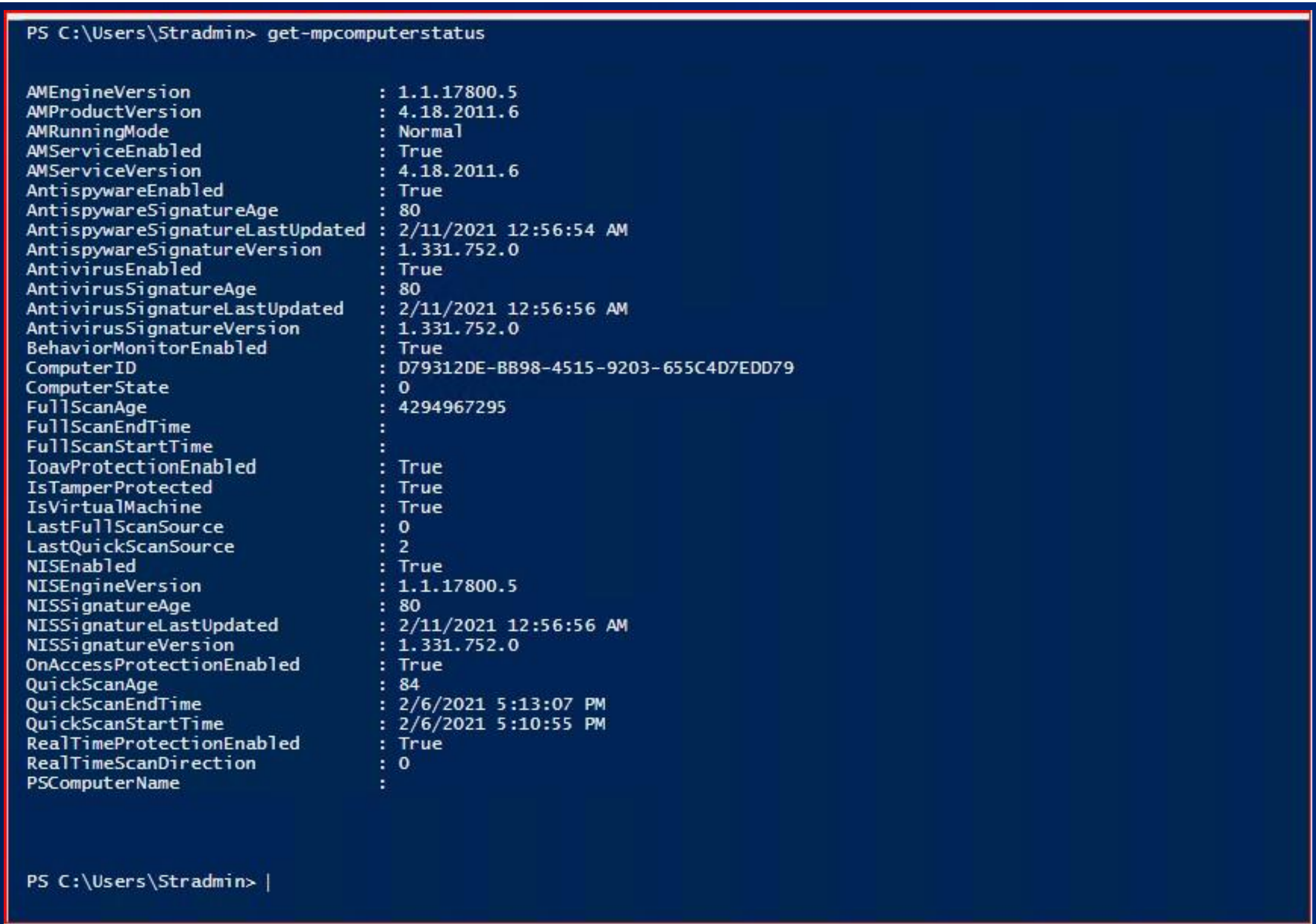
MDAV on Server 1809 and 2019

- Does NOT go into Passive Mode y default. Recommendation is to disable (PowerShell, GPO, etc.)
- Manually put into Passive Mode before migration, update definitions
- Operating systems have MSSense embedded into OS.

MDAV on Server 2016

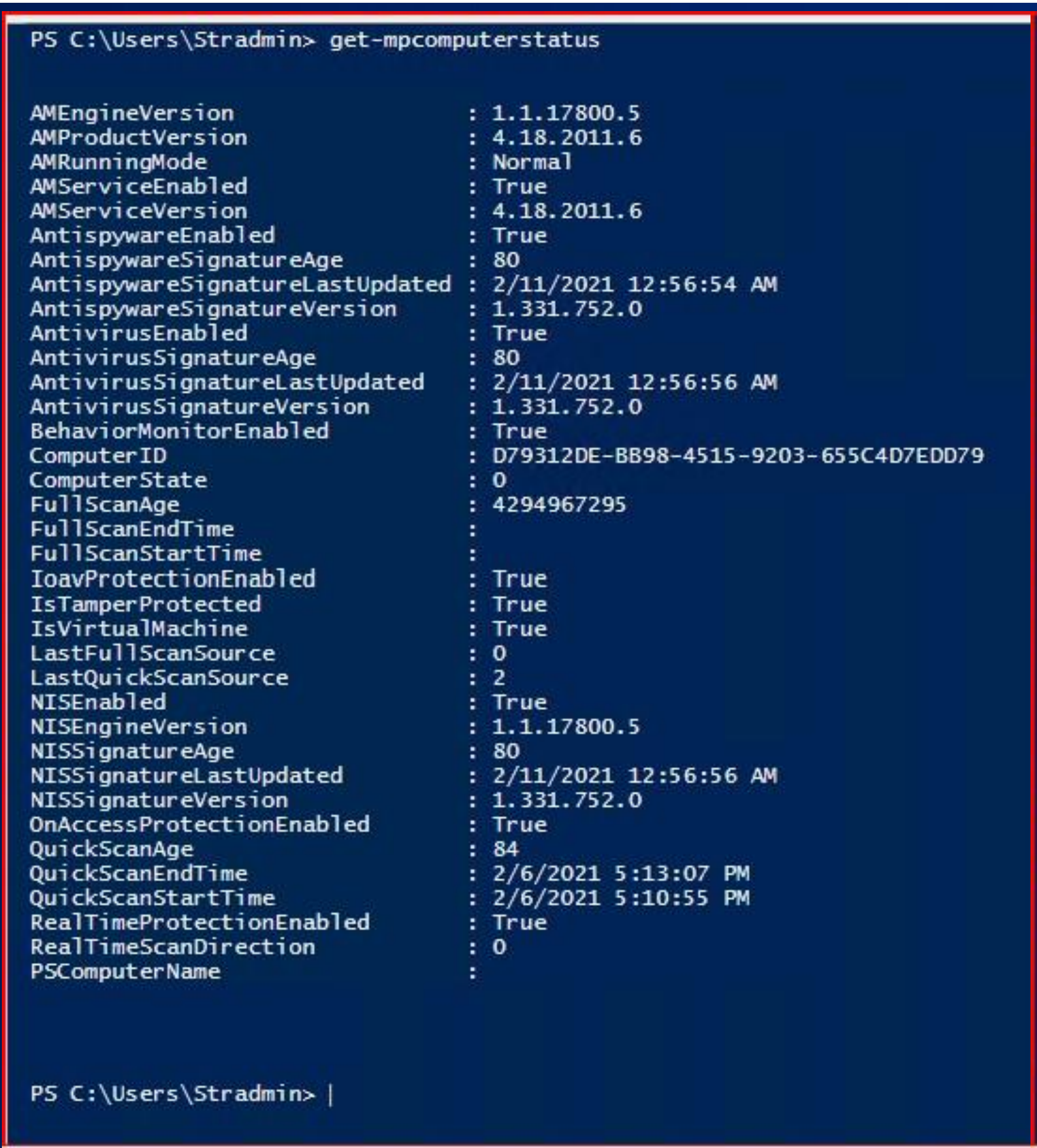
- Does NOT have Passive Mode at all. Recommendation is to disable/uninstall (PowerShell, GPO, etc.)
- No MSSense.exe- must install MMA

MDAV in Active Mode (Default)

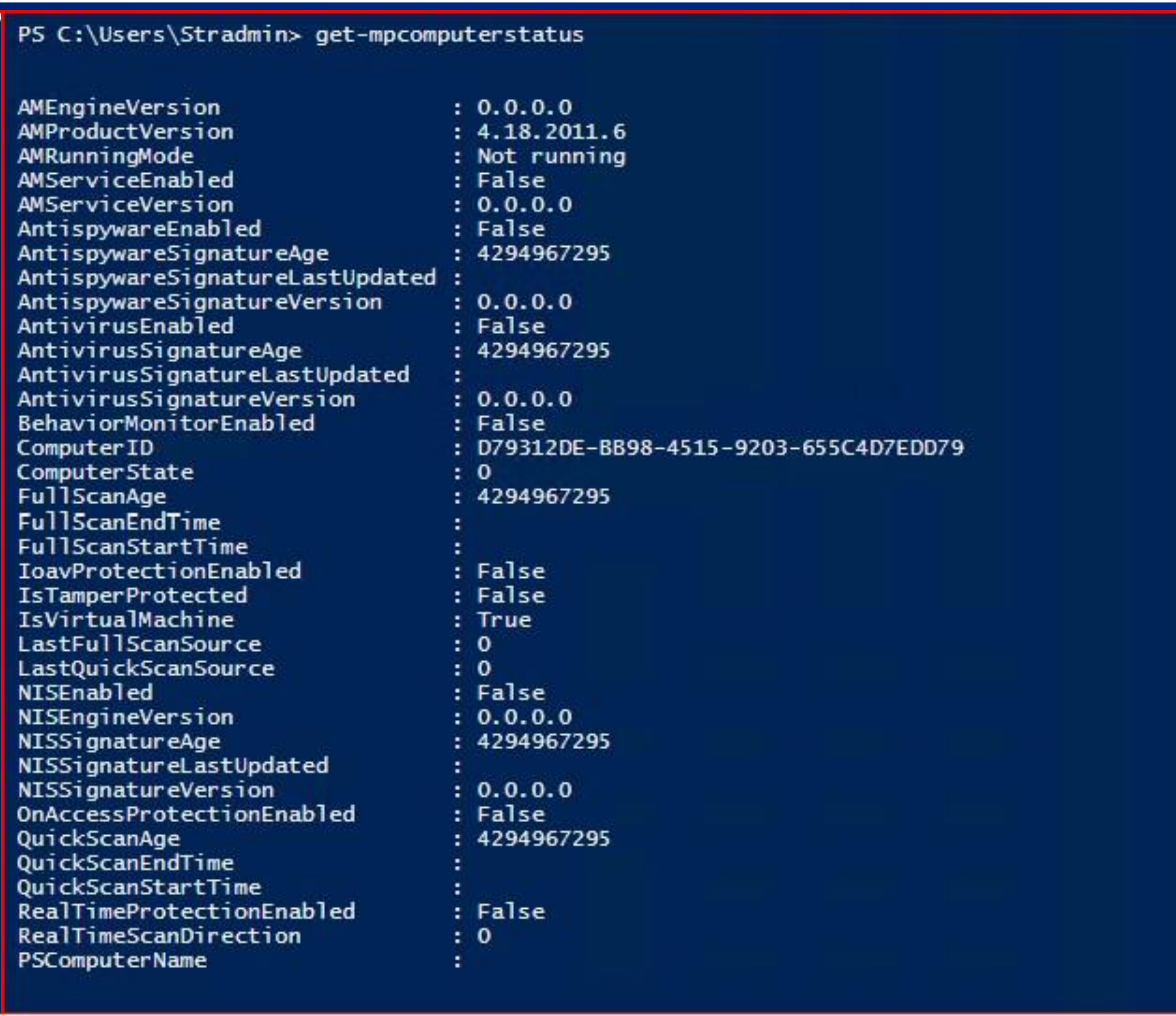


```
PS C:\Users\Stradmin> get-mpcomputerstatus


AMEngineVersion                 : 1.1.17800.5
AMProductVersion                : 4.18.2011.6
AMRunningMode                   : Normal
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2011.6
AntispywareEnabled              : True
AntispywareSignatureAge         : 80
AntispywareSignatureLastUpdated : 2/11/2021 12:56:54 AM
AntispywareSignatureVersion     : 1.331.752.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 80
AntivirusSignatureLastUpdated   : 2/11/2021 12:56:56 AM
AntivirusSignatureVersion       : 1.331.752.0
BehaviorMonitorEnabled          : True
ComputerID                      : D79312DE-BB98-4515-9203-655C4D7EDD79
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : True
IsTamperProtected               : True
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : True
NISEngineVersion                : 1.1.17800.5
NISSignatureAge                 : 80
NISSignatureLastUpdated         : 2/11/2021 12:56:56 AM
NISSignatureVersion             : 1.331.752.0
OnAccessProtectionEnabled       : True
QuickScanAge                    : 84
QuickScanEndTime                : 2/6/2021 5:13:07 PM
QuickScanStartTime              : 2/6/2021 5:10:55 PM
RealTimeProtectionEnabled       : True
RealTimeScanDirection           : 0
PSComputerName                  :



PS C:\Users\Stradmin> |
```

3rd Party AV with MDAV (self-disables by default)

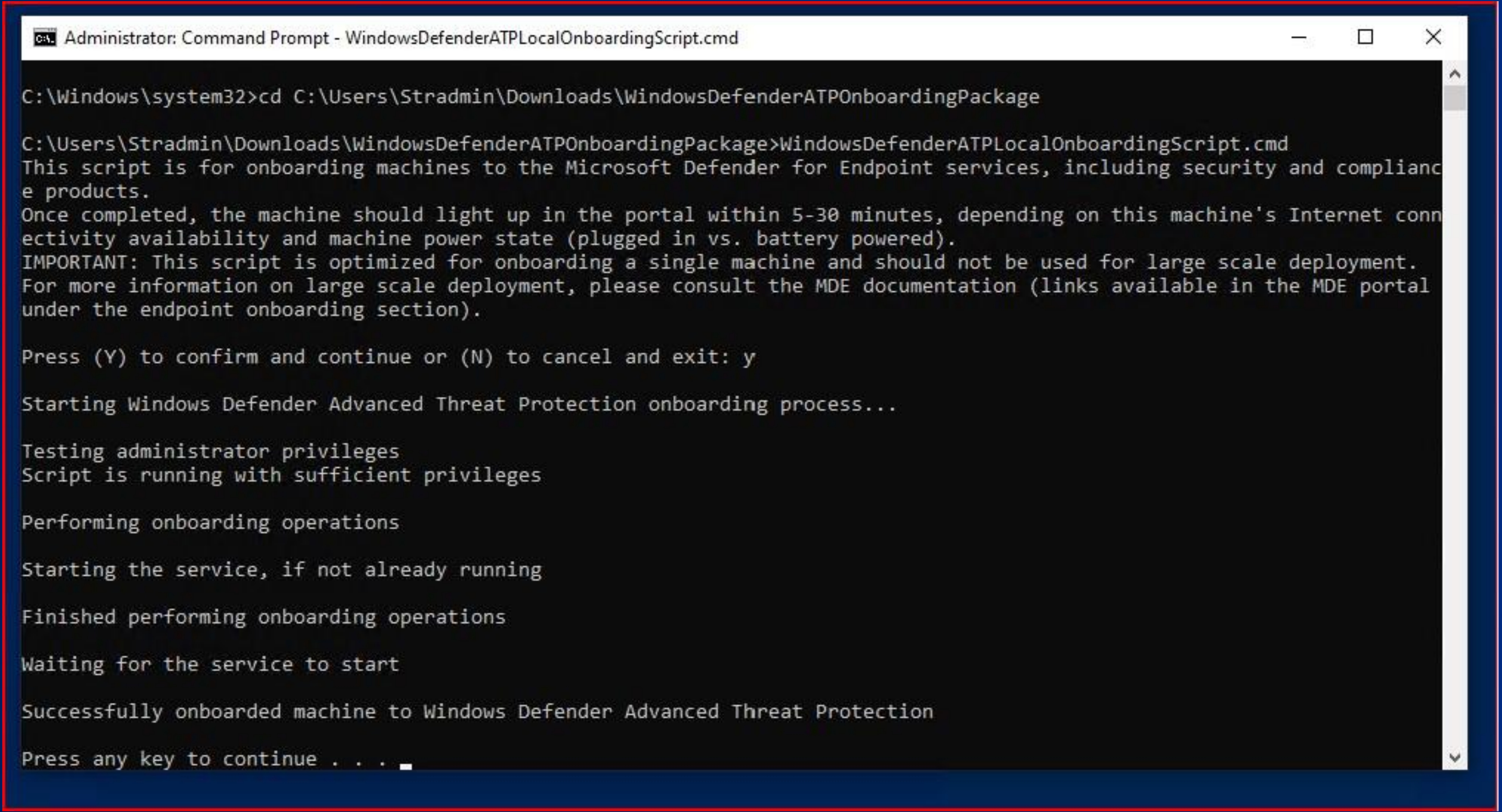


```
PS C:\Users\Stradmin> get-mpcomputerstatus


AMEngineVersion                 : 1.1.17800.5
AMProductVersion                : 4.18.2011.6
AMRunningMode                   : Normal
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2011.6
AntispywareEnabled              : True
AntispywareSignatureAge         : 80
AntispywareSignatureLastUpdated : 2/11/2021 12:56:54 AM
AntispywareSignatureVersion     : 1.331.752.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 80
AntivirusSignatureLastUpdated   : 2/11/2021 12:56:56 AM
AntivirusSignatureVersion       : 1.331.752.0
BehaviorMonitorEnabled          : True
ComputerID                      : D79312DE-BB98-4515-9203-655C4D7EDD79
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : True
IsTamperProtected               : True
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : True
NISEngineVersion                : 1.1.17800.5
NISSignatureAge                 : 80
NISSignatureLastUpdated         : 2/11/2021 12:56:56 AM
NISSignatureVersion             : 1.331.752.0
OnAccessProtectionEnabled       : True
QuickScanAge                    : 84
QuickScanEndTime                : 2/6/2021 5:13:07 PM
QuickScanStartTime              : 2/6/2021 5:10:55 PM
RealTimeProtectionEnabled       : True
RealTimeScanDirection           : 0
PSComputerName                  :



PS C:\Users\Stradmin> |
```



```
PS C:\Users\Stradmin> get-mpcomputerstatus


AMEngineVersion                 : 0.0.0.0
AMProductVersion                : 4.18.2011.6
AMRunningMode                   : Not running
AMServiceEnabled                : False
AMServiceVersion                : 0.0.0.0
AntispywareEnabled              : False
AntispywareSignatureAge         : 4294967295
AntispywareSignatureLastUpdated :
AntispywareSignatureVersion     : 0.0.0.0
AntivirusEnabled                : False
AntivirusSignatureAge           : 4294967295
AntivirusSignatureLastUpdated   :
AntivirusSignatureVersion       : 0.0.0.0
BehaviorMonitorEnabled          : False
ComputerID                      : D79312DE-BB98-4515-9203-655C4D7EDD79
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : False
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 0
NISEnabled                      : False
NISEngineVersion                : 0.0.0.0
NISSignatureAge                 : 4294967295
NISSignatureLastUpdated         :
NISSignatureVersion             : 0.0.0.0
OnAccessProtectionEnabled       : False
QuickScanAge                    : 4294967295
QuickScanEndTime                :
QuickScanStartTime              :
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
PSComputerName                  :
```

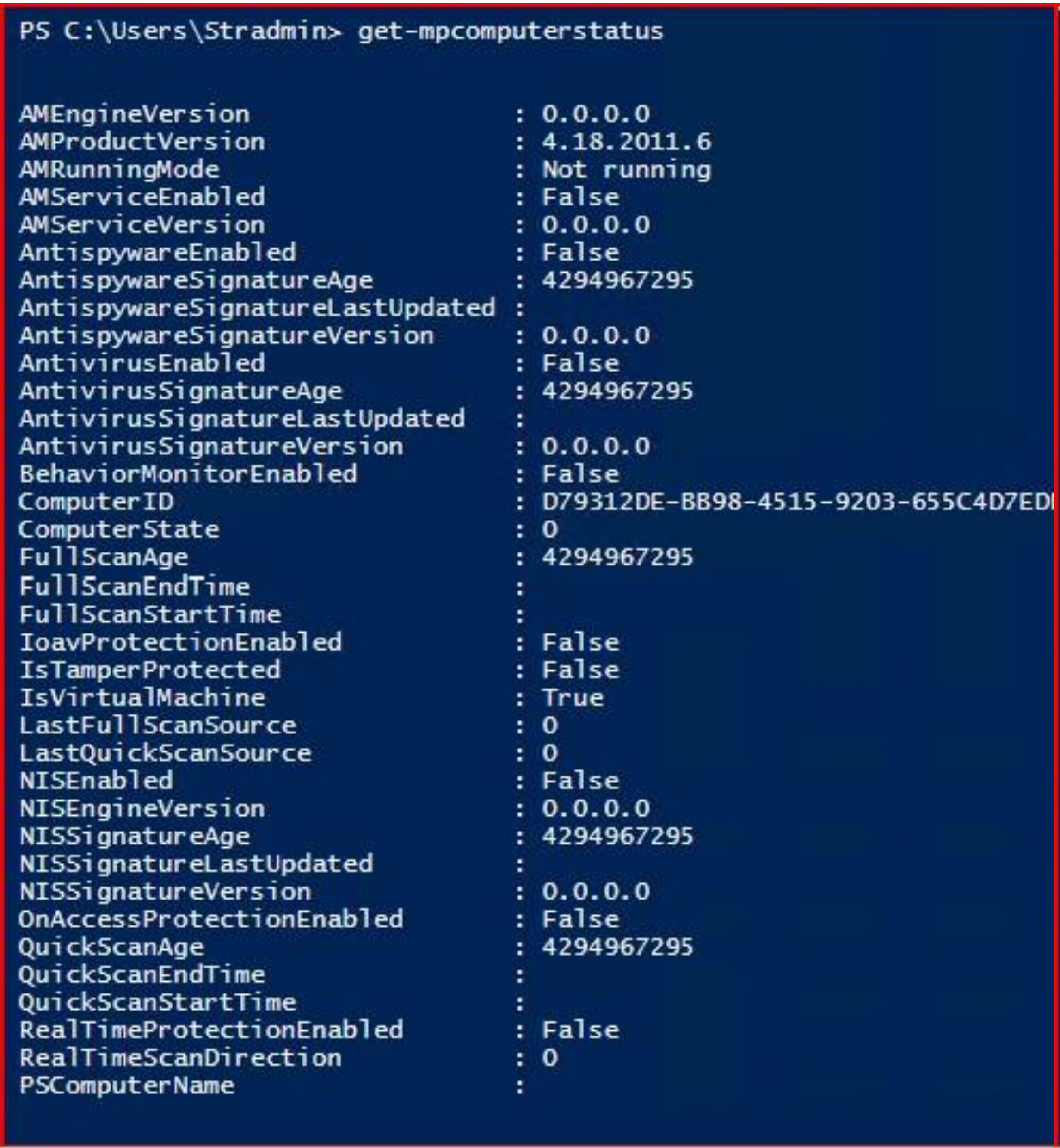
MDE Onboarding Script



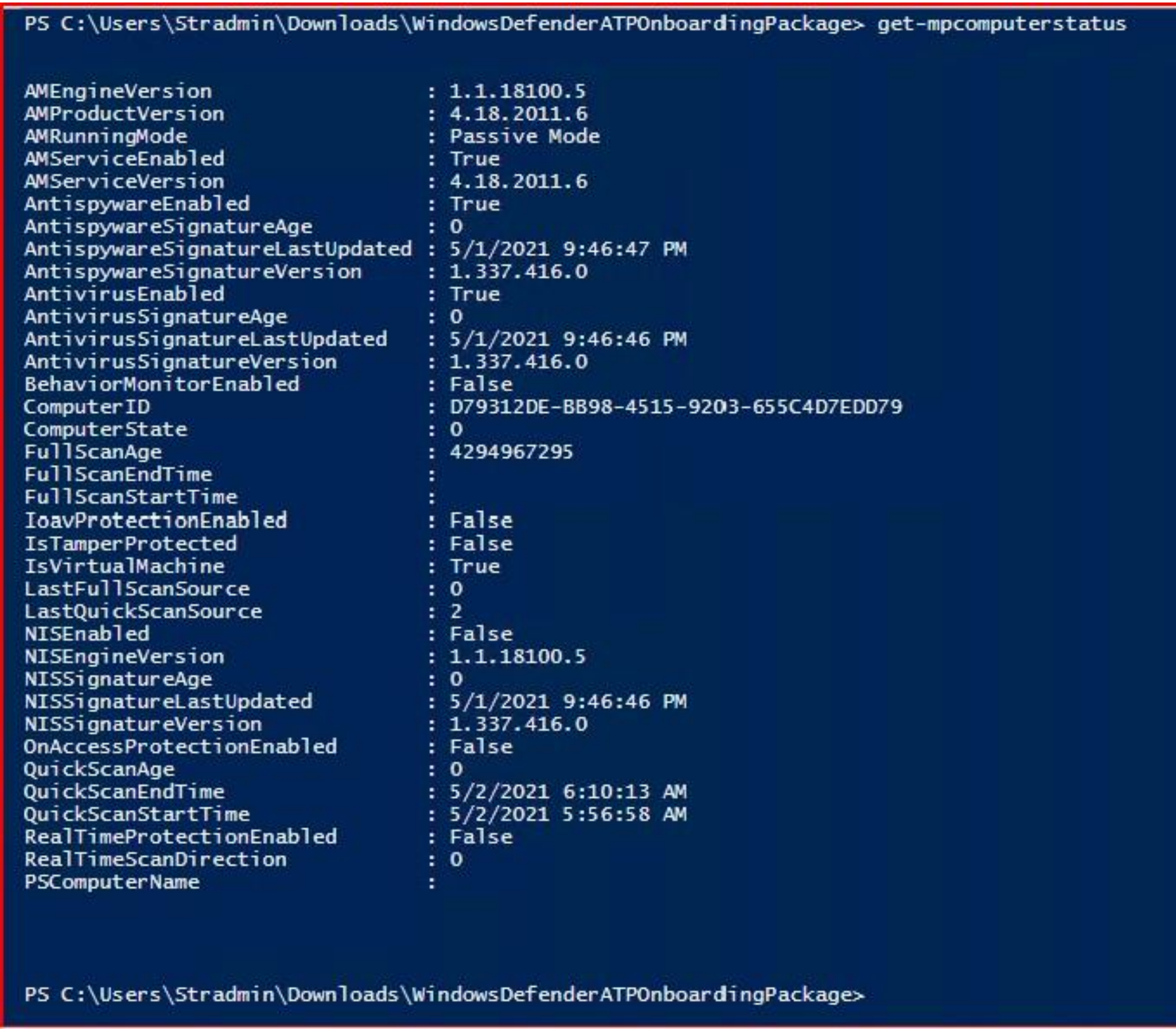
Administrator: Command Prompt - WindowsDefenderATPLocalOnboardingScript.cmd

```
C:\Windows\system32>cd C:\Users\Stradmin\Downloads\WindowsDefenderATPOnboardingPackage

C:\Users\Stradmin\Downloads\WindowsDefenderATPOnboardingPackage>WindowsDefenderATPLocalOnboardingScript.cmd
This script is for onboarding machines to the Microsoft Defender for Endpoint services, including security and complianc
e products.
Once completed, the machine should light up in the portal within 5-30 minutes, depending on this machine's Internet conn
ectivity availability and machine power state (plugged in vs. battery powered).
IMPORTANT: This script is optimized for onboarding a single machine and should not be used for large scale deployment.
For more information on large scale deployment, please consult the MDE documentation (links available in the MDE portal
under the endpoint onboarding section).

Press (Y) to confirm and continue or (N) to cancel and exit: y

Starting Windows Defender Advanced Threat Protection onboarding process...

Testing administrator privileges
Script is running with sufficient privileges

Performing onboarding operations

Starting the service, if not already running

Finished performing onboarding operations

Waiting for the service to start

Successfully onboarded machine to Windows Defender Advanced Threat Protection

Press any key to continue . . .
```

Once Onboarded MDAV goes into Passive Mode (ready for EDR Block Mode)

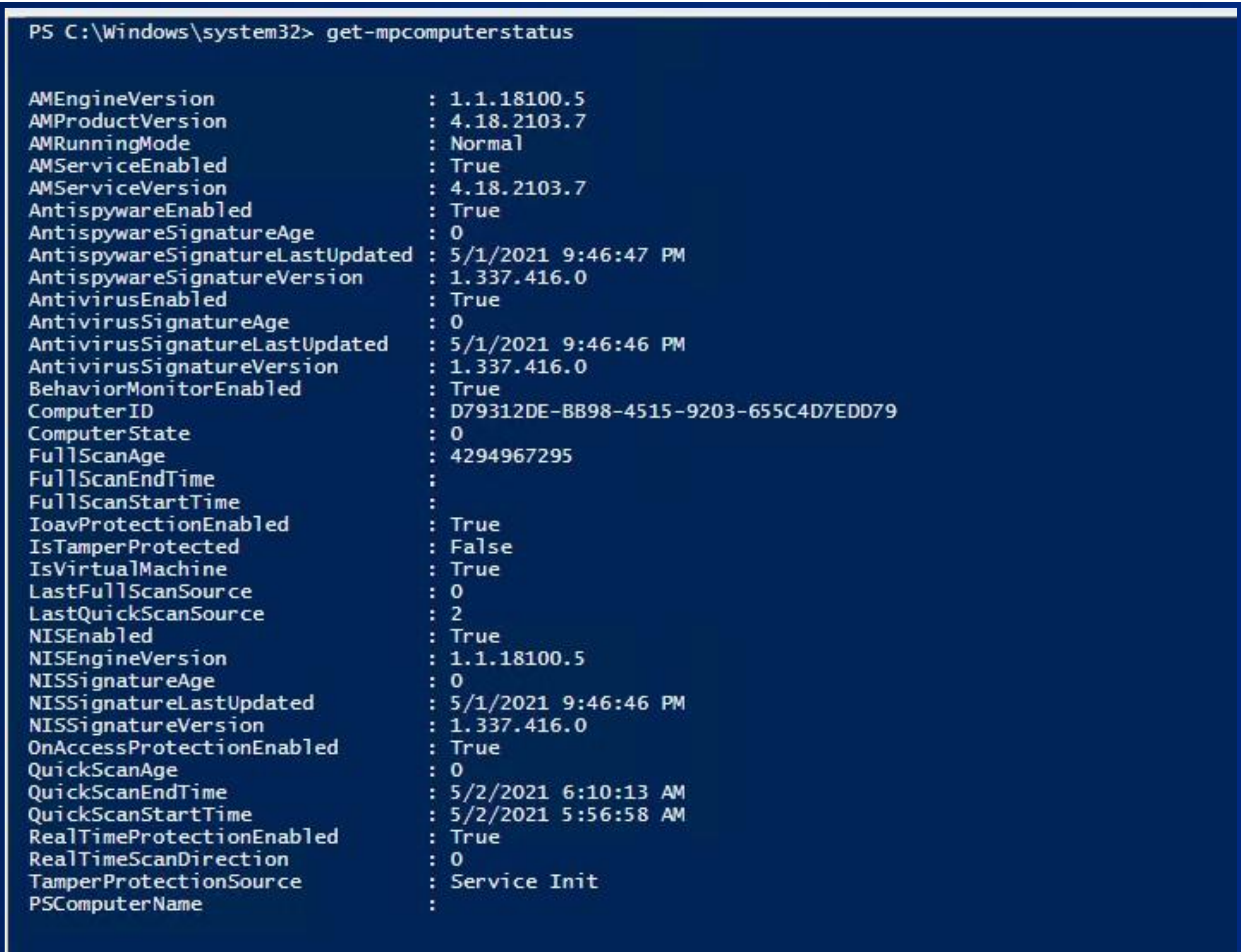


```
PS C:\Users\Stradmin> get-mpcomputerstatus


AMEngineVersion                 : 0.0.0.0
AMProductVersion                : 4.18.2011.6
AMRunningMode                   : Not running
AMServiceEnabled                : False
AMServiceVersion                : 0.0.0.0
AntispywareEnabled              : False
AntispywareSignatureAge         : 4294967295
AntispywareSignatureLastUpdated :
AntispywareSignatureVersion     : 0.0.0.0
AntivirusEnabled                : False
AntivirusSignatureAge           : 4294967295
AntivirusSignatureLastUpdated   :
AntivirusSignatureVersion       : 0.0.0.0
BehaviorMonitorEnabled          : False
ComputerID                      : D79312DE-BB98-4515-9203-655C4D7ED
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : False
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 0
NISEnabled                      : False
NISEngineVersion                : 0.0.0.0
NISSignatureAge                 : 4294967295
NISSignatureLastUpdated         :
NISSignatureVersion             : 0.0.0.0
OnAccessProtectionEnabled       : False
QuickScanAge                    : 4294967295
QuickScanEndTime                :
QuickScanStartTime              :
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
PSComputerName                  :
```



```
PS C:\Users\Stradmin\Downloads\WindowsDefenderATPOnboardingPackage> get-mpcomputerstatus


AMEngineVersion                 : 1.1.18100.5
AMProductVersion                : 4.18.2011.6
AMRunningMode                   : Passive Mode
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2011.6
AntispywareEnabled              : True
AntispywareSignatureAge         : 0
AntispywareSignatureLastUpdated : 5/1/2021 9:46:47 PM
AntispywareSignatureVersion     : 1.337.416.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 0
AntivirusSignatureLastUpdated   : 5/1/2021 9:46:46 PM
AntivirusSignatureVersion       : 1.337.416.0
BehaviorMonitorEnabled          : False
ComputerID                      : D79312DE-BB98-4515-9203-655C4D7EDD79
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : False
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : False
NISEngineVersion                : 1.1.18100.5
NISSignatureAge                 : 0
NISSignatureLastUpdated         : 5/1/2021 9:46:46 PM
NISSignatureVersion             : 1.337.416.0
OnAccessProtectionEnabled       : False
QuickScanAge                    : 0
QuickScanEndTime                : 5/2/2021 6:10:13 AM
QuickScanStartTime              : 5/2/2021 5:56:58 AM
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
PSComputerName                  :



PS C:\Users\Stradmin\Downloads\WindowsDefenderATPOnboardingPackage>
```

Reboot after uninstalling 3rd party AV

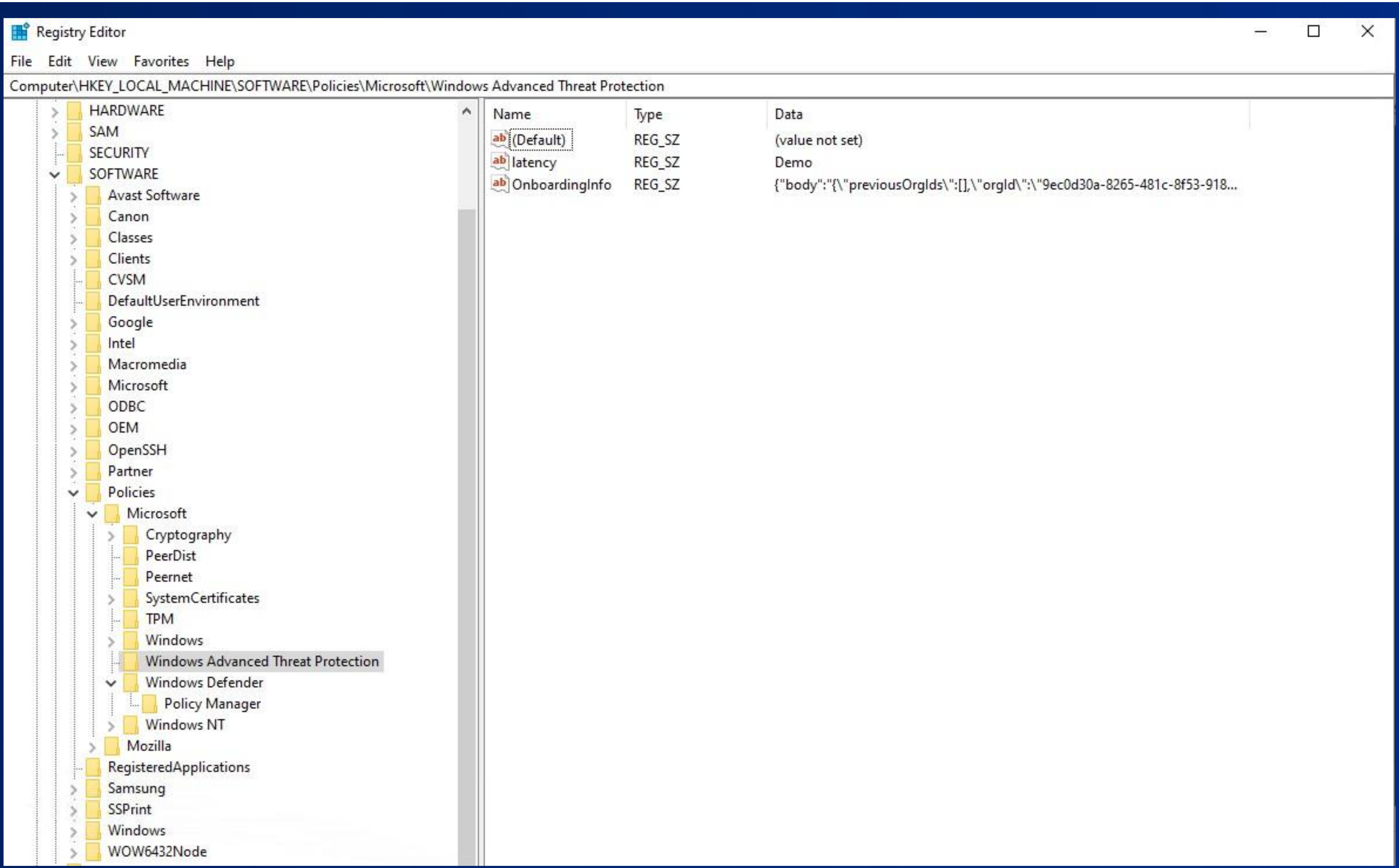


```
PS C:\Windows\system32> get-mpcomputerstatus


AMEngineVersion                 : 1.1.18100.5
AMProductVersion                : 4.18.2103.7
AMRunningMode                   : Normal
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2103.7
AntispywareEnabled              : True
AntispywareSignatureAge         : 0
AntispywareSignatureLastUpdated : 5/1/2021 9:46:47 PM
AntispywareSignatureVersion     : 1.337.416.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 0
AntivirusSignatureLastUpdated   : 5/1/2021 9:46:46 PM
AntivirusSignatureVersion       : 1.337.416.0
BehaviorMonitorEnabled          : True
ComputerID                      : D79312DE-BB98-4515-9203-655C4D7EDD79
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : True
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : True
NISEngineVersion                : 1.1.18100.5
NISSignatureAge                 : 0
NISSignatureLastUpdated         : 5/1/2021 9:46:46 PM
NISSignatureVersion             : 1.337.416.0
OnAccessProtectionEnabled       : True
QuickScanAge                    : 0
QuickScanEndTime                : 5/2/2021 6:10:13 AM
QuickScanStartTime              : 5/2/2021 5:56:58 AM
RealTimeProtectionEnabled       : True
RealTimeScanDirection           : 0
TamperProtectionSource          : Service Init
PSComputerName                  :
```

Migration Process with Windows 10 with active 3rd party AV

- *Set AV Exclusions in MDE as Indicators
- * Add MDAV exclusions to 3rd party AV
- Configure Antimalware policies (SCCM, GPO, Intune, etc.)
- Onboard device to MDE, this will put MDAV into Passive Mode and wake up SENSE service
- Update MDAV Engine and definitions
- Remove 3rd party AV
- Run Detection Script to ensure MDAV is reporting alerts to MDE

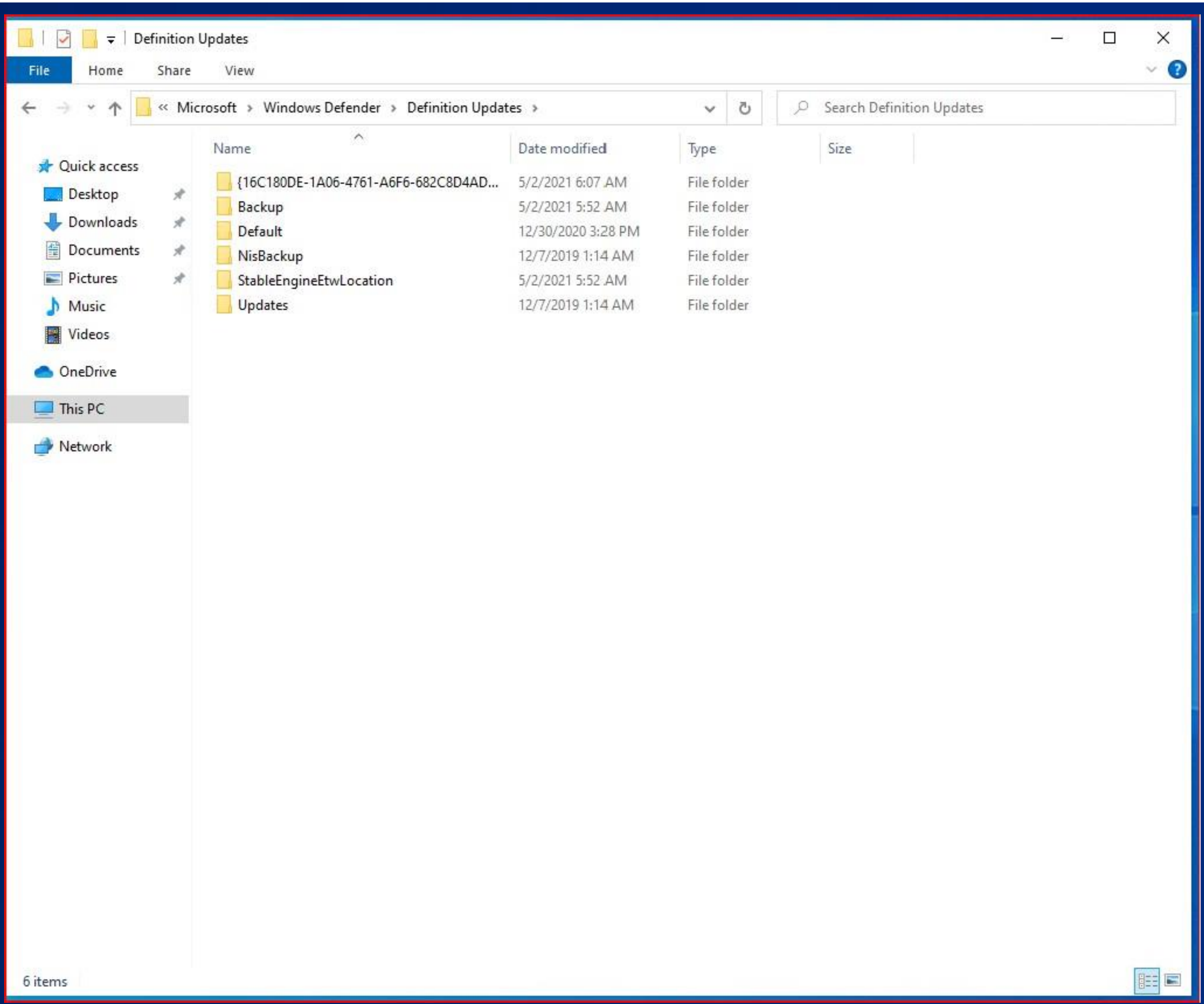
MDE writes to registry- org id, workspace id and key (encrypted)



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection

Name	Type	Data
(Default)	REG_SZ	(value not set)
latency	REG_SZ	Demo
OnboardingInfo	REG_SZ	{"body":"{\"previousOrgIds\":[],\"orgId\":\"9ec0d30a-8265-481c-8f53-918...

Filepath for MDAV- C:\ProgramData\Microsoft\Windows Defender

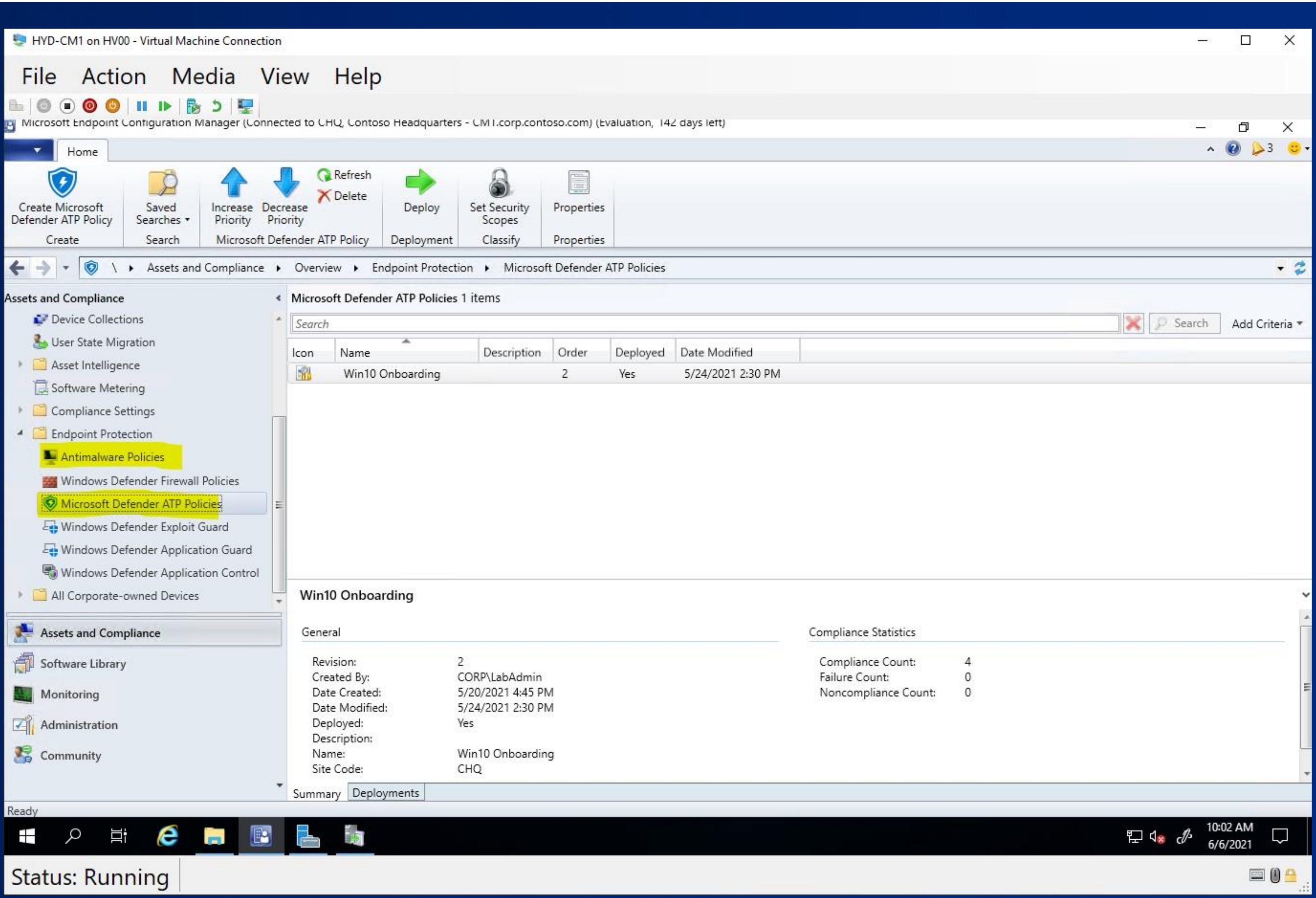


Name	Date modified	Type	Size
{16C180DE-1A06-4761-A6F6-682C8D4AD...	5/2/2021 6:07 AM	File folder	
Backup	5/2/2021 5:52 AM	File folder	
Default	12/30/2020 3:28 PM	File folder	
NisBackup	12/7/2019 1:14 AM	File folder	
StableEngineEtwLocation	5/2/2021 5:52 AM	File folder	
Updates	12/7/2019 1:14 AM	File folder	

Migration Process with SCEP with active 3rd party AV

- Configure antimalware policies and Exclusions
- Onboard device with MMA
- Remove 3rd party AV
- Install SCEP
- Reboot
- Run detection script

Onboarding Win 10 to MDE via SCCM Policy


HYD-CM1 on HV00 - Virtual Machine Connection
File
Action
Media
View
Help
Microsoft Endpoint Configuration Manager (Connected to CHQ, Contoso Headquarters - CM1.corp.contoso.com) (Evaluation, 142 days left)
Home
3
Create Microsoft Defender ATP Policy
Create
Saved Searches
Search
Increase Priority
Decrease Priority
Refresh
Delete
Microsoft Defender ATP Policy
Deploy
Deployment
Set Security Scopes
Classify
Properties
Properties
\ ▸ Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Microsoft Defender ATP Policies
Assets and Compliance
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Defender Firewall Policies
Microsoft Defender ATP Policies
Windows Defender Exploit Guard
Windows Defender Application Guard
Windows Defender Application Control
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Community
Search
Search
Add Criteria
Summary
Deployments
Ready
10:02 AM
6/6/2021
Status: Running

Microsoft Defender ATP Policies 1 items

Icon	Name	Description	Order	Deployed	Date Modified
	Win10 Onboarding		2	Yes	5/24/2021 2:30 PM

Win10 Onboarding

General

Revision: 2
Created By: CORP\LabAdmin
Date Created: 5/20/2021 4:45 PM
Date Modified: 5/24/2021 2:30 PM
Deployed: Yes
Description:
Name: Win10 Onboarding
Site Code: CHQ

Compliance Statistics

Compliance Count: 4
Failure Count: 0
Noncompliance Count: 0

Custom SCCM Task Sequence

Rob-Strawley/Migrate2MDAV: Automated Migration from 3rd party AV to Microsoft Defender AV (github.com)

Demo

- Onboarding scripts from Portal
- Antimalware policies
- Onboard MDE Policy (.onboarding)
- Task Sequence

Migration Process with Server 2016

- Install MMA- verify onboarding in MDE
- Uninstall 3rd party AV
- Reboot
- Install-WindowsFeature -Name Windows-Defender
- Reboot
- Get-mpcomputerstatus
- Test Detection Script

Summary

- MDE is an enhanced EDR on Windows 10 1709 and above
- Different migration procedures for various scenarios. No authoritative process for down-level Operating Systems.
- Understand how MDE AIR works and why it isn't supported on various Windows 10 Builds.
- Understand the necessary URLs to walk customer through complex network configurations.
- Onboard devices to MDE first when possible

Gotchas (Symantec)

- No vendor provided “Ripper” tool
- Use PowerShell WMI-

```
(Get-WmiObject -Class Win32_Product -Filter "Name='Symantec Endpoint
Protection'" -ComputerName . ).Uninstall()
```

- Can use offline update file (mpam-fe.exe) during troubleshooting.

Questions?

Microsoft