**Default Antivirus settings**

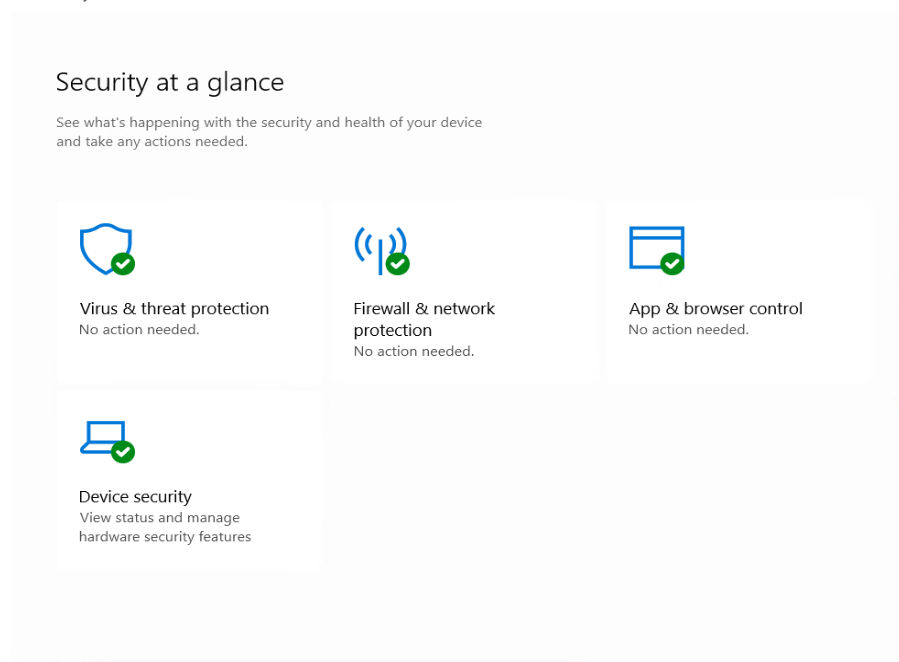
Users can not make changes to Antivirus policy

Below is demonstrated by logging as a regular domain user

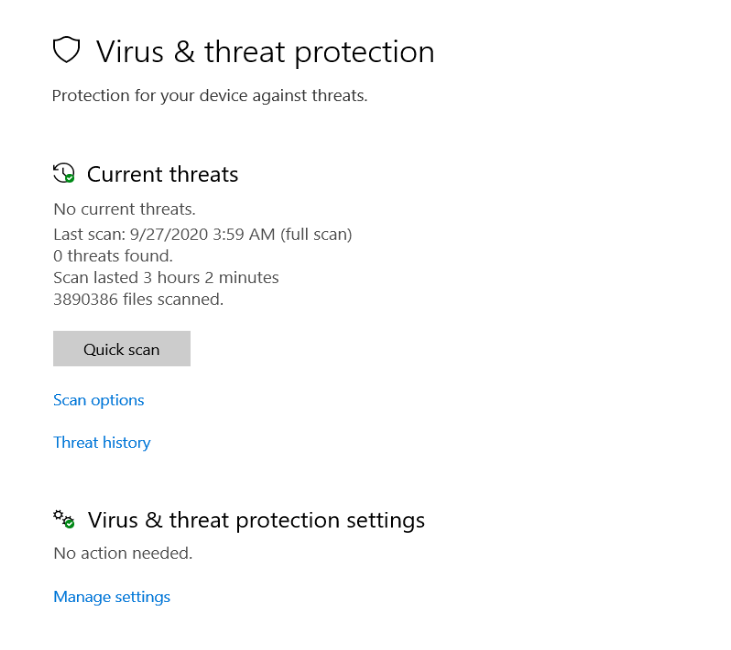
**This pop up screen pop for every section below. Regular domain users will get his prompt for each section.**



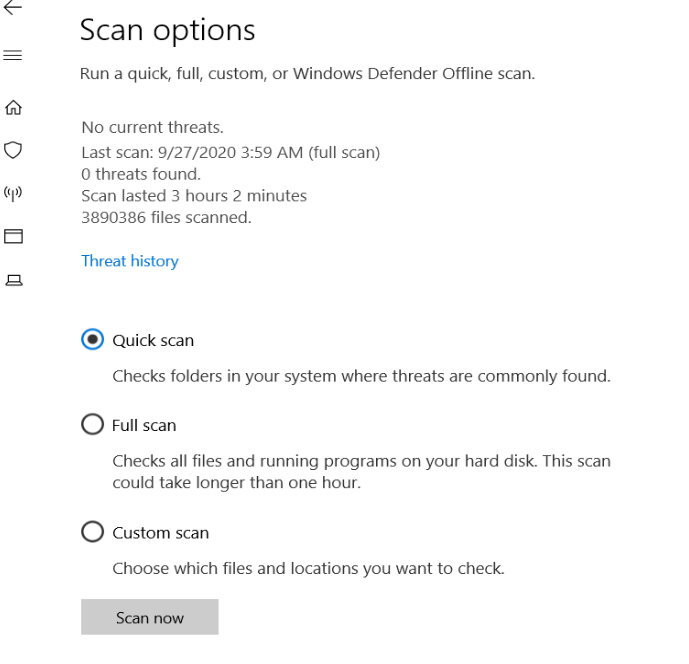
**Below is logged on as a Domain Administrator. Only Domain Administrators can make changes**



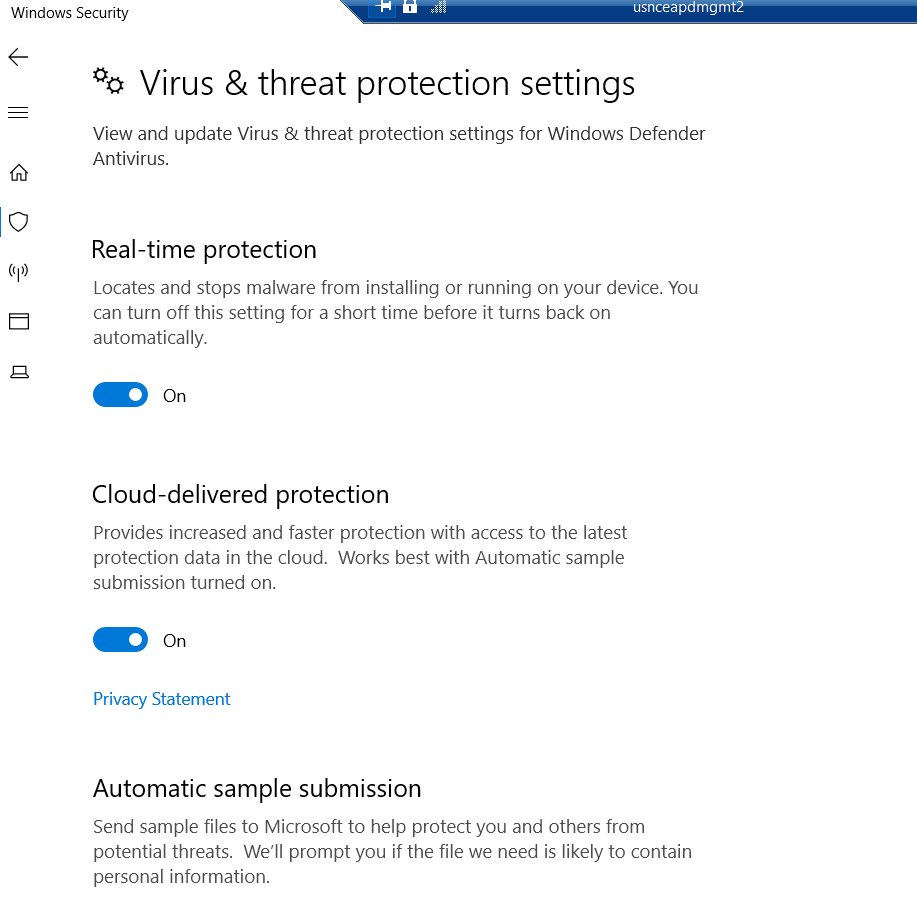
**Options As Domain Administrator**



**More Options As Administrator**



**Even More As Domain Administrator**



**Current Default Settings:**

**Below is the exported configuration with screenshots:**

AMEngineVersion : 1.1.17400.5

AMProductVersion : 4.18.2008.9

AMRunningMode : Normal

AMServiceEnabled : True

AMServiceVersion : 4.18.2008.9

AntispywareEnabled : True

AntispywareSignatureAge : 0

AntispywareSignatureLastUpdated : 9/27/2020 1:34:42 PM

AntispywareSignatureVersion : 1.323.2054.0

AntivirusEnabled : True

AntivirusSignatureAge : 0

AntivirusSignatureLastUpdated : 9/27/2020 1:34:44 PM

AntivirusSignatureVersion : 1.323.2054.0

BehaviorMonitorEnabled : True

ComputerID : 2EDDA6FE-1C7F-A695-D18E-3777EDFCF82A

ComputerState : 0

FullScanAge : 1

FullScanEndTime : 9/27/2020 7:01:17 AM

FullScanStartTime : 9/27/2020 3:59:08 AM

IoavProtectionEnabled : True

IsTamperProtected : False

IsVirtualMachine : True

LastFullScanSource : 2

LastQuickScanSource : 0

NISEnabled : True

NISEngineVersion : 1.1.17400.5

NISSignatureAge : 0

NISSignatureLastUpdated : 9/27/2020 1:34:44 PM

NISSignatureVersion : 1.323.2054.0

OnAccessProtectionEnabled : True

QuickScanAge : 4294967295

QuickScanEndTime :

QuickScanStartTime :

RealTimeProtectionEnabled : True

RealTimeScanDirection : 0

PSComputerName :

AllowNetworkProtectionOnWinServer : False

AttackSurfaceReductionOnlyExclusions :

AttackSurfaceReductionRules\_Actions : {1, 1, 1, 1...}

AttackSurfaceReductionRules\_Ids : {26190899-1602-49e8-8b27-eb1d0a1ce869,

3b576869-a4ec-4529-8536-b80a7769e899,

5beb7efe-fd9a-4556-801d-275e5ffc04cc,

9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2...}

CheckForSignaturesBeforeRunningScan : False

CloudBlockLevel : 1

CloudExtendedTimeout : 1

ComputerID : 2EDDA6FE-1C7F-A695-D18E-3777EDFCF82A

ControlledFolderAccessAllowedApplications :

ControlledFolderAccessProtectedFolders :

DisableArchiveScanning : False

DisableAutoExclusions : False

DisableBehaviorMonitoring : False

DisableBlockAtFirstSeen : False

DisableCatchupFullScan : True

DisableCatchupQuickScan : True

DisableCpuThrottleOnIdleScans :

DisableDatagramProcessing : False

DisableEmailScanning : False

DisableIntrusionPreventionSystem :

DisableIOAVProtection : False

DisablePrivacyMode : False

DisableRealtimeMonitoring : False

DisableRemovableDriveScanning : False

DisableRestorePoint : True

DisableScanningMappedNetworkDrivesForFullScan : True

DisableScanningNetworkFiles : False

DisableScriptScanning : False

EnableControlledFolderAccess : 0

EnableFileHashComputation : False

EnableLowCpuPriority : False

EnableNetworkProtection : 1

ExclusionExtension :

ExclusionIpAddress :

ExclusionPath : {C:\Program Files (x86)\FireEye\xagt\xagt.exe, C:\Program Files

(x86)\Tanium\Tanium Client\TaniumClient.exe, C:\program

files\Microsoft Monitoring

Agent\agent\HealthService.exeMonitoringHost.exe, C:\Program

Files\Microsoft Monitoring Agent\Agent\MonitoringHost.exe...}

ExclusionProcess :

HighThreatDefaultAction : 0

LowThreatDefaultAction : 0

MAPSReporting : 2

MeteredConnectionUpdates : False

ModerateThreatDefaultAction : 0

PUAProtection : 1

QuarantinePurgeItemsAfterDelay : 90

RandomizeScheduleTaskTimes : True

RealTimeScanDirection : 0

RemediationScheduleDay : 0

RemediationScheduleTime : 02:00:00

ReportingAdditionalActionTimeOut : 10080

ReportingCriticalFailureTimeOut : 10080

ReportingNonCriticalTimeOut : 1440

ScanAvgCPULoadFactor : 50

ScanOnlyIfIdleEnabled : True

ScanParameters : 2

ScanPurgeItemsAfterDelay : 15

ScanScheduleDay : 1

ScanScheduleQuickScanTime : 00:00:00

ScanScheduleTime : 02:00:00

SevereThreatDefaultAction : 0

SharedSignaturesPath :

SignatureAuGracePeriod : 0

SignatureBlobFileSharesSources :

SignatureBlobUpdateInterval : 60

SignatureDefinitionUpdateFileSharesSources :

SignatureDisableUpdateOnStartupWithoutEngine : False

SignatureFallbackOrder : MicrosoftUpdateServer|MMPC

SignatureFirstAuGracePeriod : 120

SignatureScheduleDay : 8

SignatureScheduleTime : 01:45:00

SignatureUpdateCatchupInterval : 1

SignatureUpdateInterval : 0

SubmitSamplesConsent : 1

ThreatIDDefaultAction\_Actions :

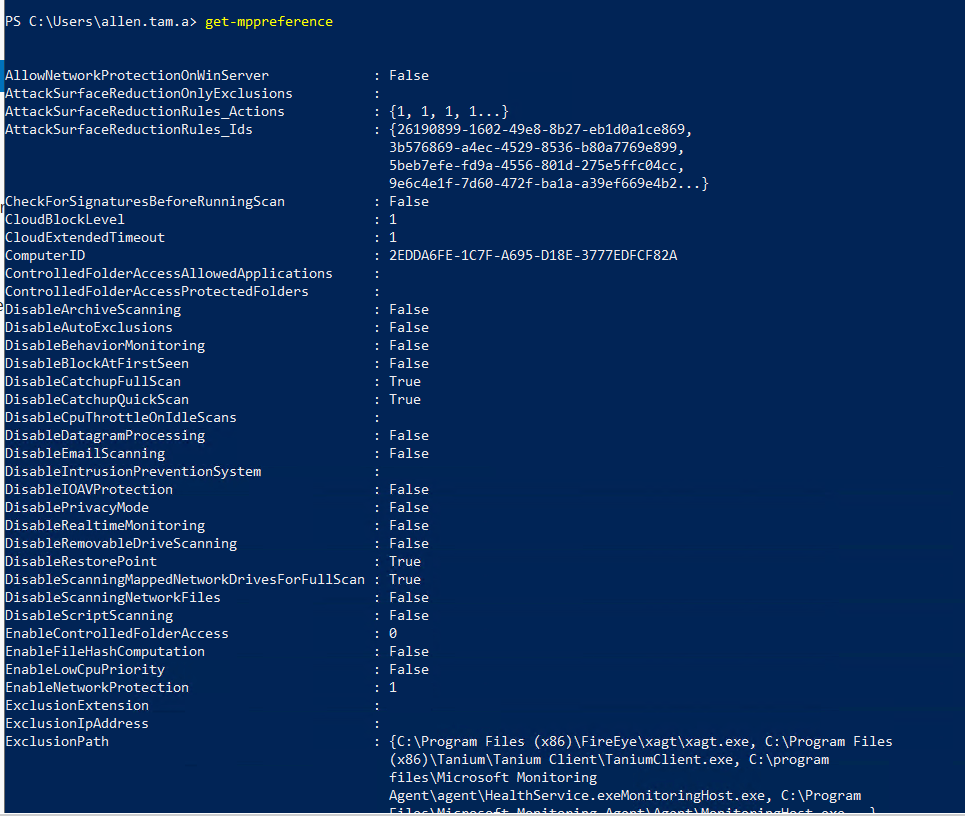
ThreatIDDefaultAction\_Ids :

UILockdown : False

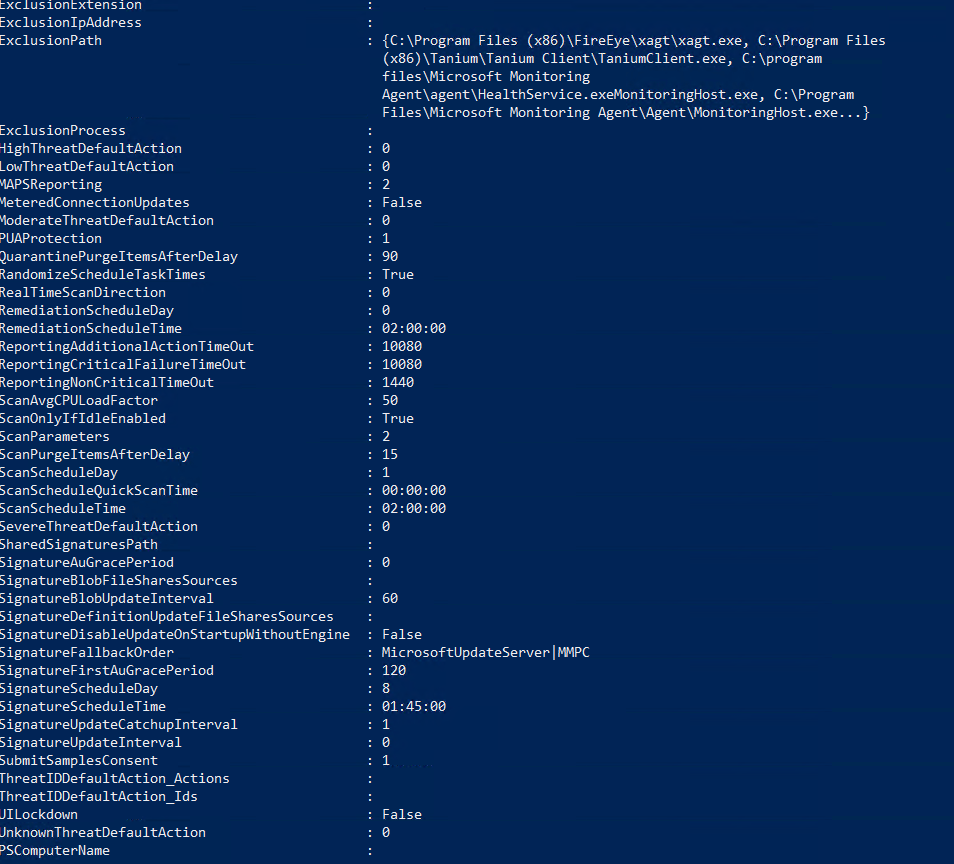
UnknownThreatDefaultAction : 0

PSComputerName :

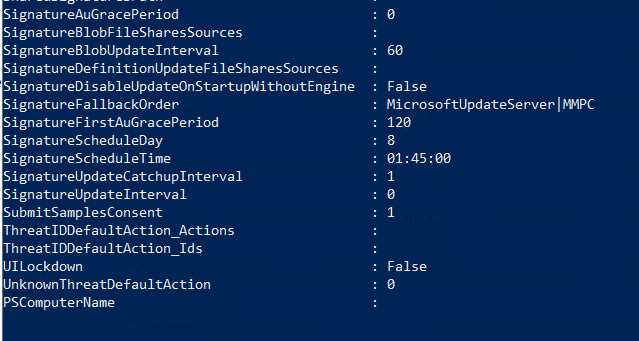
**Screenshot1**



**Screenshot 2**



**Screenshot 3**



**Group policy Settings**

