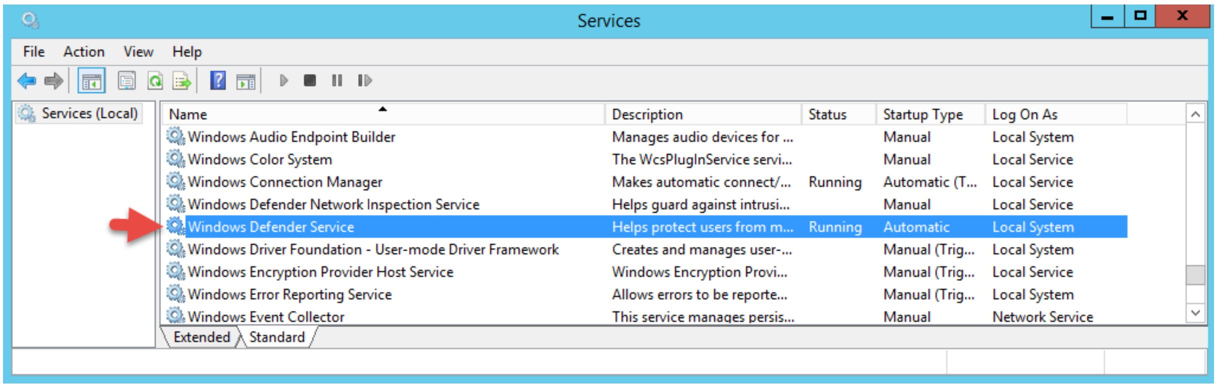
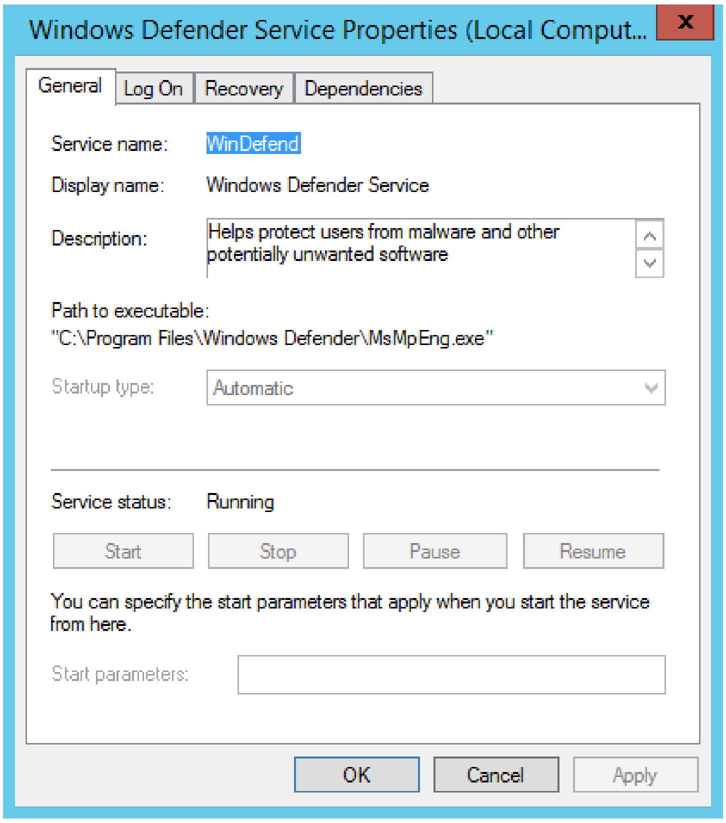
Windows Server 10 - Windows Defender

Windows Server 10 bekommt weitere Boardmittel in puncto Sicherheit implementiert. Der **Windows Defender** (Malware Protection) ist nun Bestandteil der neuen Server Versionen.

Nach der Installation von Server 10 ist der Dienst bereist aktiv. Die GUI muss aber nach installiert werden, ansonsten bleibt zur Konfiguration nur die Kommandozeile übrig.



Name	Description	Status	Startup Type	Log On As
Windows Audio Endpoint Builder	Manages audio devices for ...		Manual	Local System
Windows Color System	The WcsPlugInService servi...		Manual	Local Service
Windows Connection Manager	Makes automatic connect/...	Running	Automatic (T...	Local Service
Windows Defender Network Inspection Service	Helps guard against intrusi...		Manual	Local Service
Windows Defender Service	Helps protect users from m...	Running	Automatic	Local System
Windows Driver Foundation - User-mode Driver Framework	Creates and manages user-...		Manual (Trig...	Local System
Windows Encryption Provider Host Service	Windows Encryption Provi...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows errors to be reporte...		Manual (Trig...	Local System
Windows Event Collector	This service manages persis...		Manual	Network Service



Service name: WinDefend

Display name: Windows Defender Service

Description: Helps protect users from malware and other potentially unwanted software

Path to executable:
"C:\Program Files\Windows Defender\MsMpEng.exe"

Startup type: Automatic

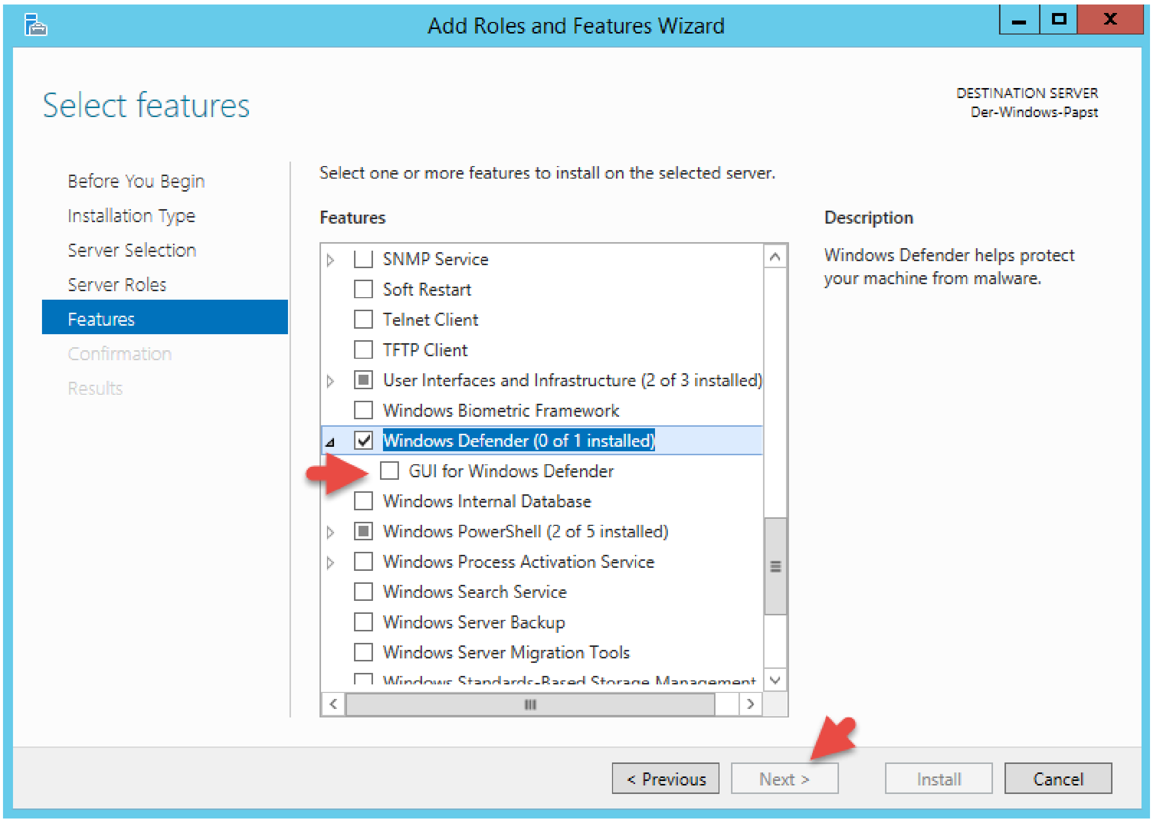
Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Die GUI lässt sich über **Manage Roles and Features** nachträglich installieren.

Windows Server 10 - Windows Defender



Select features

DESTINATION SERVER
Der-Windows-Papst

Select one or more features to install on the selected server.

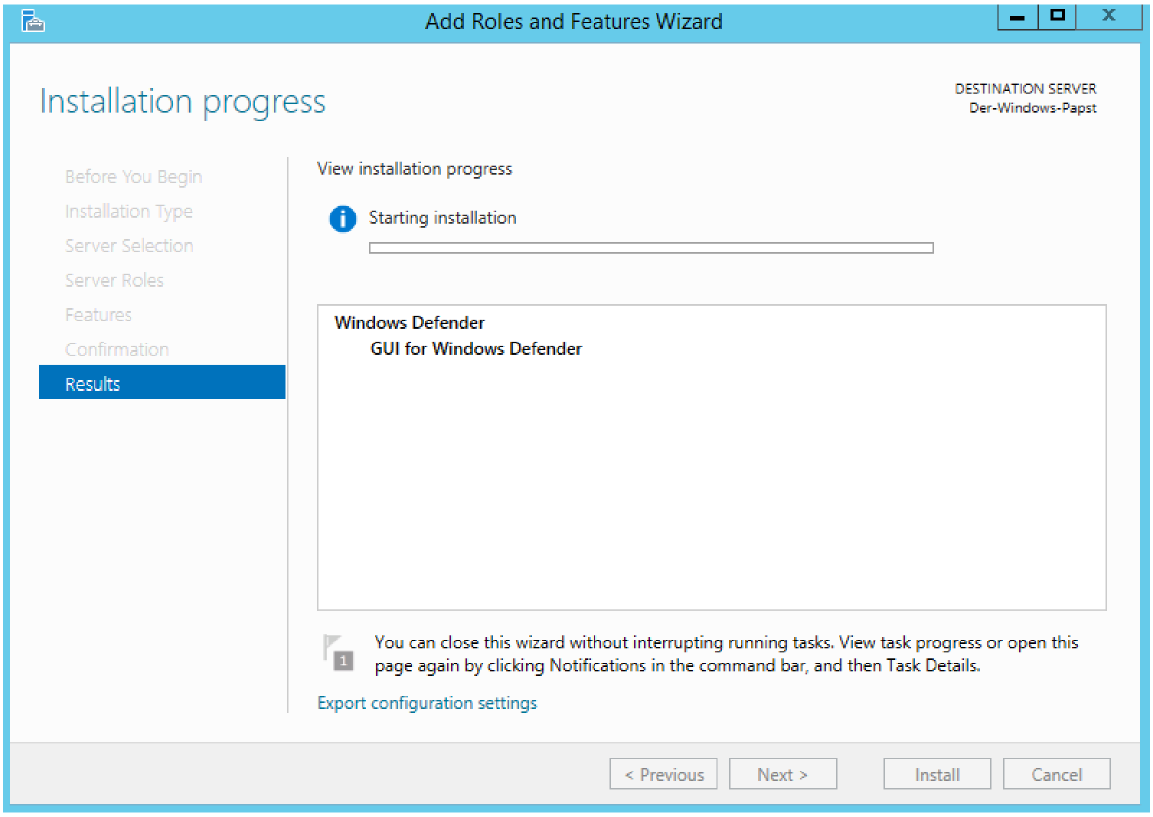
Features

- □ SNMP Service
- □ Soft Restart
- □ Telnet Client
- □ TFTP Client
- ▣ User Interfaces and Infrastructure (2 of 3 installed)
- □ Windows Biometric Framework
- ☑ Windows Defender (0 of 1 installed)
  - □ GUI for Windows Defender
- □ Windows Internal Database
- ▣ Windows PowerShell (2 of 5 installed)
- □ Windows Process Activation Service
- □ Windows Search Service
- □ Windows Server Backup
- □ Windows Server Migration Tools
- □ Windows Standards-Based Storage Management

Description

Windows Defender helps protect your machine from malware.

Checkbox > Next



Installation progress

DESTINATION SERVER
Der-Windows-Papst

View installation progress

Starting installation

Windows Defender
GUI for Windows Defender

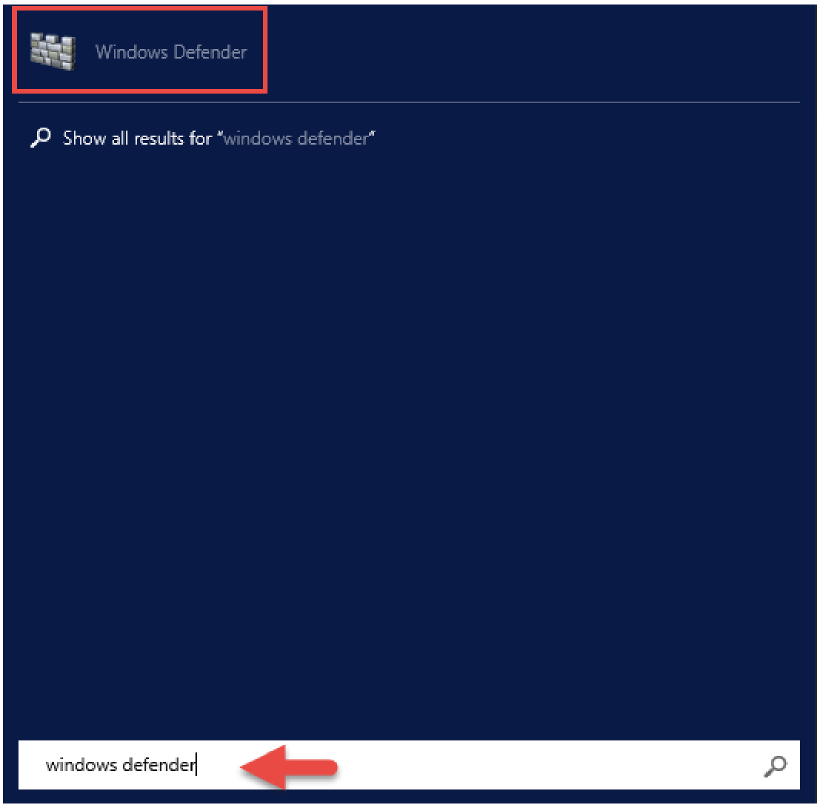
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

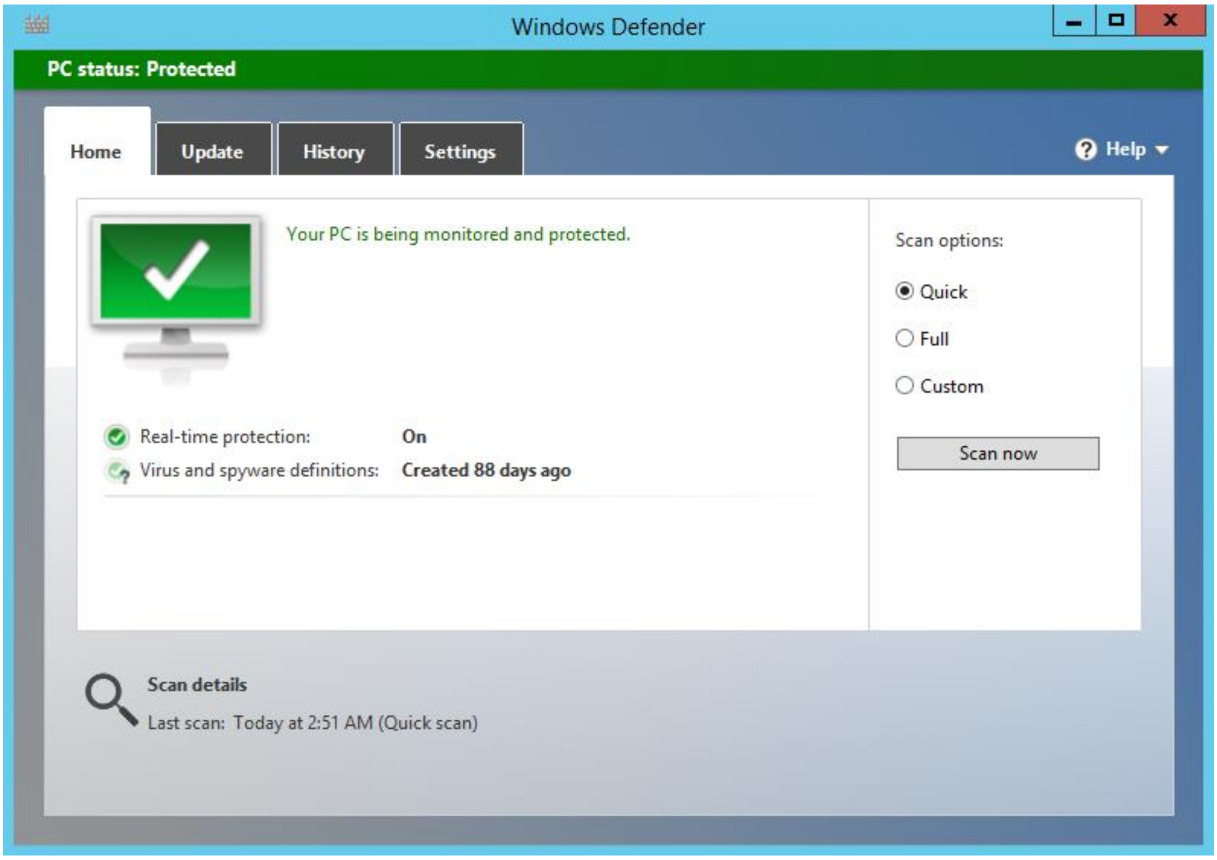
Export configuration settings

Erstellt von Jörn Walter www.der-windows-papst.de – 01.10.2014

Windows Server 10 - Windows Defender

Wie gewohnt rufen wir die GUI über **Start > Search** auf.





PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Created 88 days ago

Scan options:

● Quick

○ Full

○ Custom

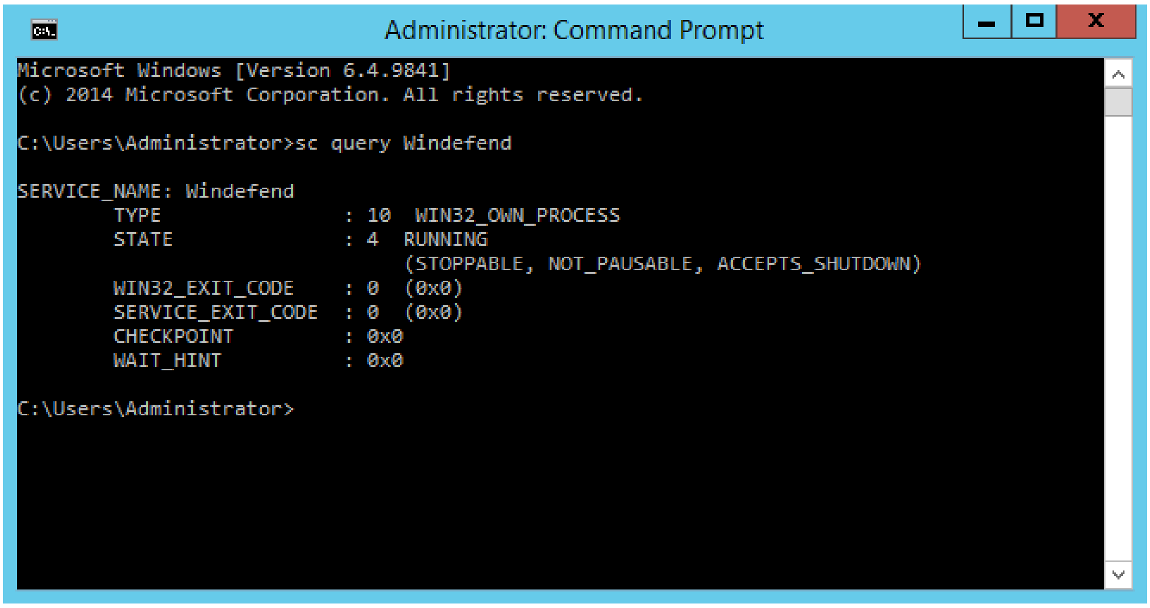
Scan details

Last scan: Today at 2:51 AM (Quick scan)

Windows Server 10 - Windows Defender

Über die Kommandozeile können wir den Dienststatus wie folgt abfragen:

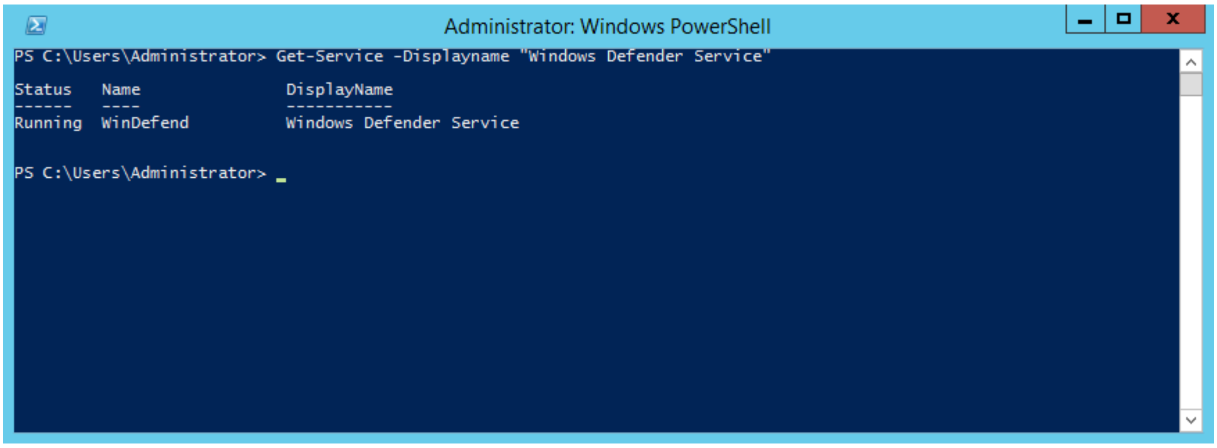
sc query Windefend



```
Microsoft Windows [Version 6.4.9841]
(c) 2014 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>sc query Windefend

SERVICE_NAME: Windefend
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\Administrator>
```

Über Powershell lässt sich der Status mit folgendem Befehl abfragen:

Get-Service –Displayname „Windows Defender Service“



```
PS C:\Users\Administrator> Get-Service -Displayname "Windows Defender Service"

Status   Name               DisplayName
------   ----               -----------
Running  WinDefend          Windows Defender Service


PS C:\Users\Administrator> _
```

Mit diesem Befehl lässt sich das Live Monitoring deaktivieren:

Set-MpPreference -DisableRealtimeMonitoring $true

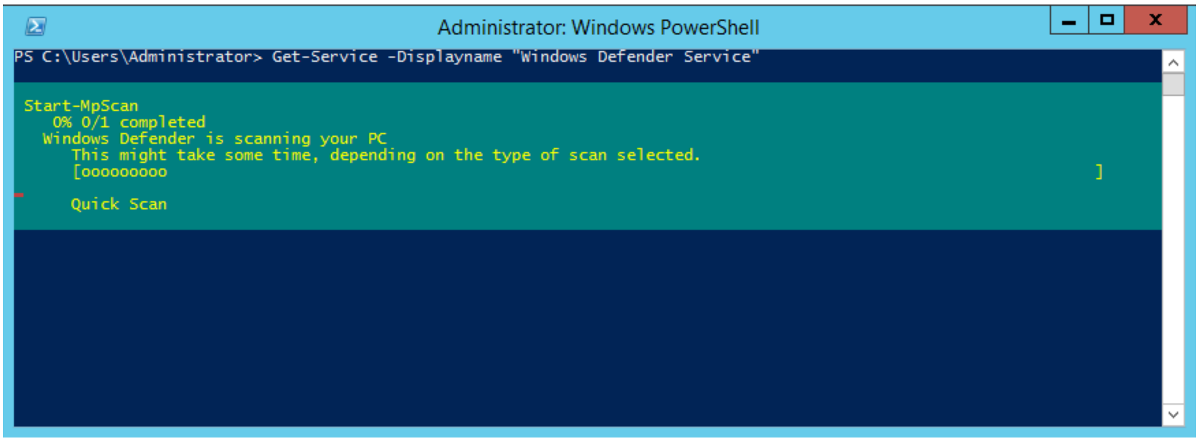
Mit diesem Befehl lässt sich das Live Monitoring aktivieren:

Set-MpPreference -DisableRealtimeMonitoring $false

Windows Server 10 - Windows Defender

Mit diesem Befehl starten wir den Windows Defender QuickScan:

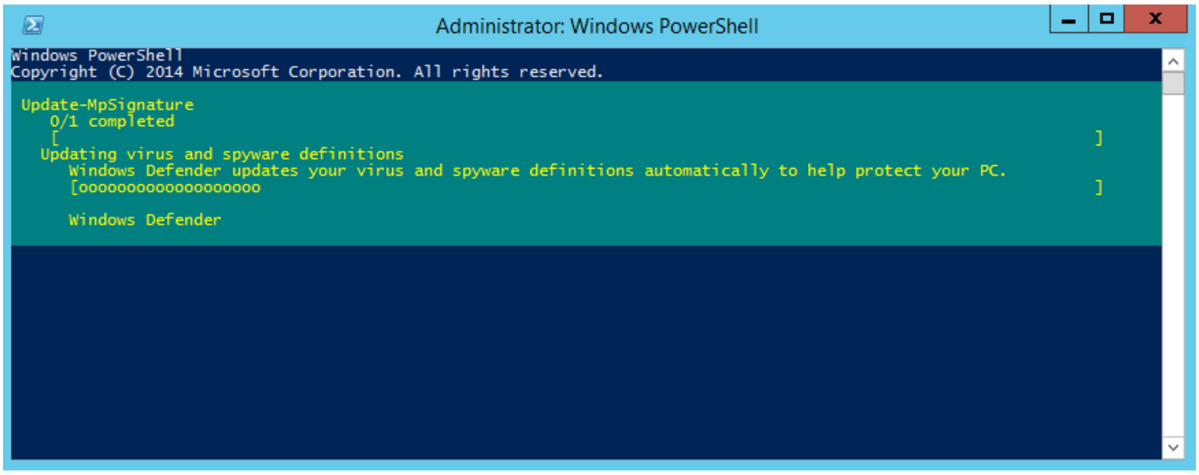
Start-MpScan



```
PS C:\Users\Administrator> Get-Service -Displayname "Windows Defender Service"

 Start-MpScan
    0% 0/1 completed
   Windows Defender is scanning your PC
      This might take some time, depending on the type of scan selected.
      [ooooooooo                                                                                          ]

      Quick Scan
```

Mit diesem Befehl starten wir das Update der Antimalware Signatur:

Update-MpSignature

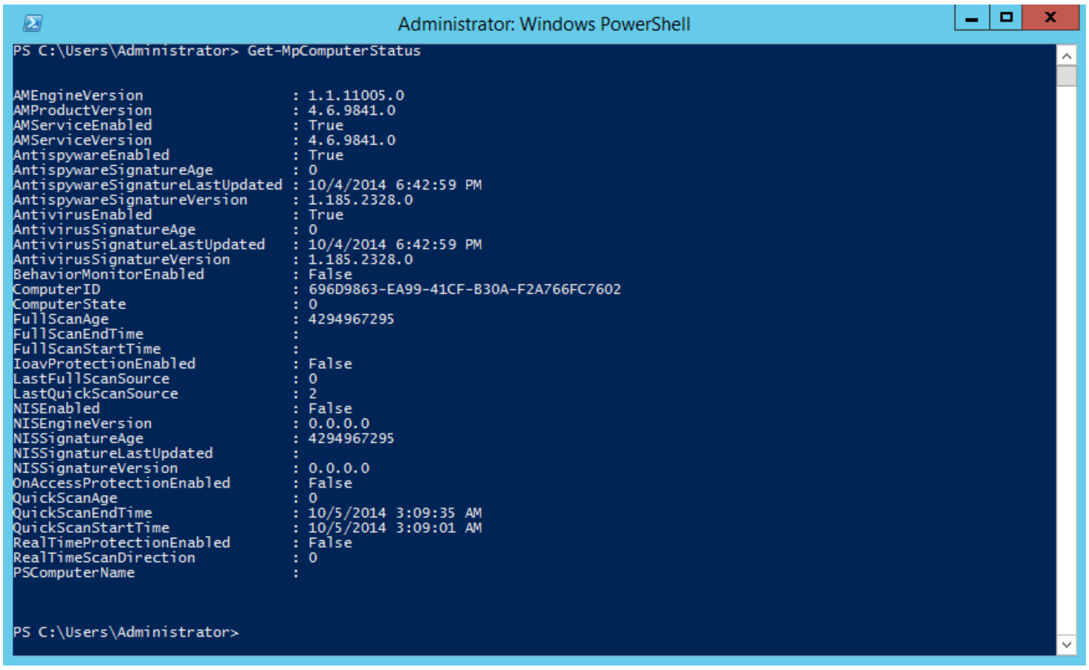


```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

 Update-MpSignature
    0/1 completed
    [                                                                                                      ]
   Updating virus and spyware definitions
      Windows Defender updates your virus and spyware definitions automatically to help protect your PC.
      [oooooooooooooooooooo                                                                                ]

      Windows Defender
```

Windows Server 10 - Windows Defender

Mit diesem Befehl bekommen wir den Status angezeigt:

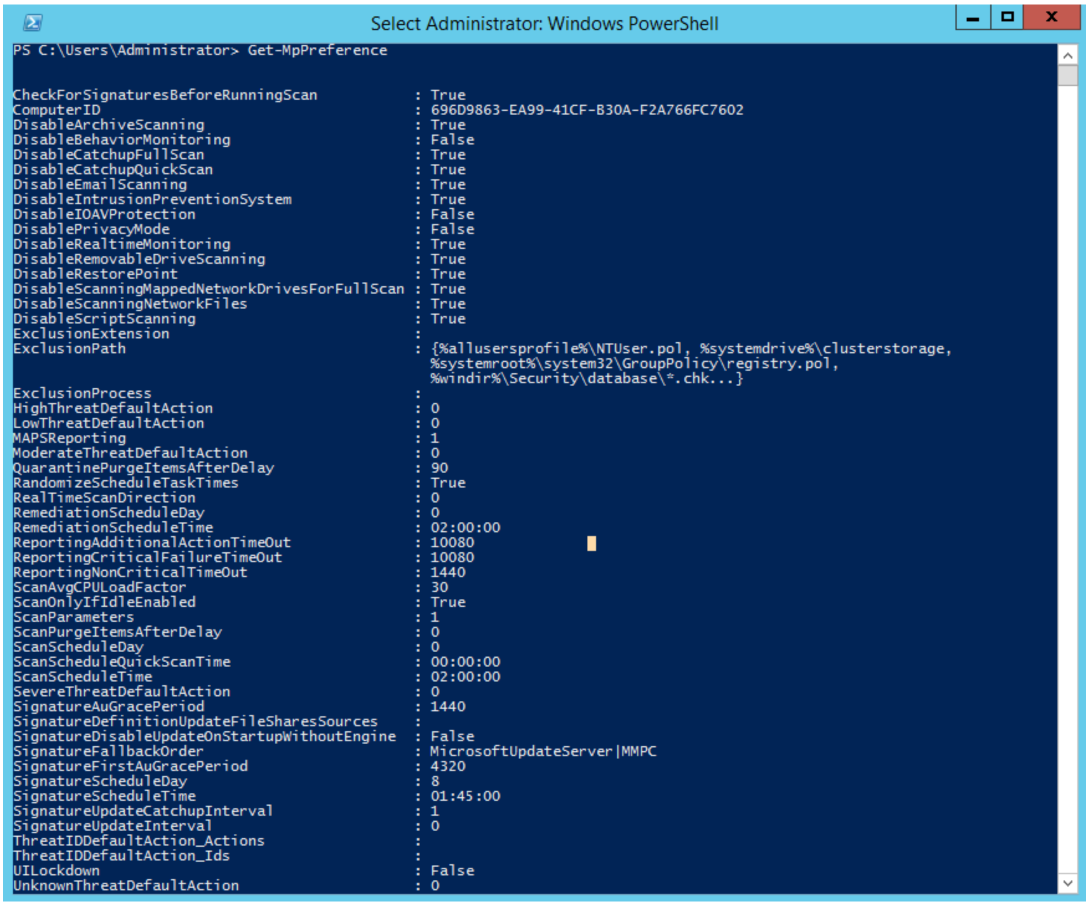
Get-MpComputerStatus



```
PS C:\Users\Administrator> Get-MpComputerStatus


AMEngineVersion                 : 1.1.11005.0
AMProductVersion                : 4.6.9841.0
AMServiceEnabled                : True
AMServiceVersion                : 4.6.9841.0
AntispywareEnabled              : True
AntispywareSignatureAge         : 0
AntispywareSignatureLastUpdated : 10/4/2014 6:42:59 PM
AntispywareSignatureVersion     : 1.185.2328.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 0
AntivirusSignatureLastUpdated   : 10/4/2014 6:42:59 PM
AntivirusSignatureVersion       : 1.185.2328.0
BehaviorMonitorEnabled          : False
ComputerID                      : 696D9863-EA99-41CF-B30A-F2A766FC7602
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : False
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : False
NISEngineVersion                : 0.0.0.0
NISSignatureAge                 : 4294967295
NISSignatureLastUpdated         :
NISSignatureVersion             : 0.0.0.0
OnAccessProtectionEnabled       : False
QuickScanAge                    : 0
QuickScanEndTime                : 10/5/2014 3:09:35 AM
QuickScanStartTime              : 10/5/2014 3:09:01 AM
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
PSComputerName                  :



PS C:\Users\Administrator>
```

Mit diesem Befehl lassen wir uns die Einstellungen anzeigen:

Get-MpPreference



```
PS C:\Users\Administrator> Get-MpPreference


CheckForSignaturesBeforeRunningScan           : True
ComputerID                                    : 696D9863-EA99-41CF-B30A-F2A766FC7602
DisableArchiveScanning                        : True
DisableBehaviorMonitoring                     : False
DisableCatchupFullScan                        : True
DisableCatchupQuickScan                       : True
DisableEmailScanning                          : True
DisableIntrusionPreventionSystem              : True
DisableIOAVProtection                         : False
DisablePrivacyMode                            : False
DisableRealtimeMonitoring                     : True
DisableRemovableDriveScanning                 : True
DisableRestorePoint                           : True
DisableScanningMappedNetworkDrivesForFullScan : True
DisableScanningNetworkFiles                   : True
DisableScriptScanning                         : True
ExclusionExtension                            :
ExclusionPath                                 : {%allusersprofile%\NTUser.pol, %systemdrive%\clusterstorage,
                                                %systemroot%\system32\GroupPolicy\registry.pol,
                                                %windir%\Security\database\*.chk...}
ExclusionProcess                              :
HighThreatDefaultAction                       : 0
LowThreatDefaultAction                        : 0
MAPSReporting                                 : 1
ModerateThreatDefaultAction                   : 0
QuarantinePurgeItemsAfterDelay                : 90
RandomizeScheduleTaskTimes                    : True
RealTimeScanDirection                         : 0
RemediationScheduleDay                        : 0
RemediationScheduleTime                       : 02:00:00
ReportingAdditionalActionTimeOut              : 10080
ReportingCriticalFailureTimeOut               : 10080
ReportingNonCriticalTimeOut                   : 1440
ScanAvgCPULoadFactor                          : 30
ScanOnlyIfIdleEnabled                         : True
ScanParameters                                : 1
ScanPurgeItemsAfterDelay                      : 0
ScanScheduleDay                               : 0
ScanScheduleQuickScanTime                     : 00:00:00
ScanScheduleTime                              : 02:00:00
SevereThreatDefaultAction                     : 0
SignatureAuGracePeriod                        : 1440
SignatureDefinitionUpdateFileSharesSources    :
SignatureDisableUpdateOnStartupWithoutEngine  : False
SignatureFallbackOrder                        : MicrosoftUpdateServer|MMPC
SignatureFirstAuGracePeriod                   : 4320
SignatureScheduleDay                          : 8
SignatureScheduleTime                         : 01:45:00
SignatureUpdateCatchupInterval                : 1
SignatureUpdateInterval                       : 0
ThreatIDDefaultAction_Actions                 :
ThreatIDDefaultAction_Ids                     :
UILockdown                                    : False
UnknownThreatDefaultAction                    : 0
```