Build Report for WS-01

**Report type:** Basic

**Inventory date:** 21/11/2020 21:33

**Inventory script:** Get-Win10Info.ps1

**Run by:** AD\administrator

[Registry] Operating System 4

[Registry] Installed Programs (System) 5

[WMI] Operating System 6

[WMI] Computer System 7

[WMI] Windows System Assessment Tool 8

[WMI] Network Adapter Configuration 9

[WMI] Physical Memory 10

[WMI] Processor 11

[WMI] Logical Disk 12

[WMI] Disk Partition 13

[WMI] Share 14

[WMI] Start Up Command 15

[WMI] Page File Usage 16

[WMI] Quick Fix Engineering (Updates) 17

[WMI] System Enclosure 18

[WMI] Boot Configuration 19

[WMI] BIOS 20

[WMI] User Accounts 21

[WMI] Groups 22

[WMI] Group Membership 23

[WMI] System Accounts 24

[WMI] Time Zone 25

[WMI] Registry 26

[WMI] Environment 27

[WMI] CD ROM Drive 32

[WMI] Video Controller 33

[WMI] Sound Device 34

[WMI] Printers 35

[WMI] Disk Drive 36

[WMI] Encryptable Volume 37

[WMI] Firewall Product 38

[WMI] Antivirus Product 39

[WMI] Antispyware Product 40

[WMI] Optional Features 41

[System] Computer Certificates 42

# [Registry] Operating System

This data is collected from the registry key (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion)

| Item | Value |
| --- | --- |
| Product Name | Windows 10 Enterprise |
| Edition ID | Enterprise |
| Build | 19042.508 |
| Build Branch | vb\_release |
| Version | 2009 |
| Registered Organisation |  |
| Registered Owner | GR |

Table 1: [Registry] Operating System

# [Registry] Installed Programs (System)

This data is collected from the Windows Registry subkeys HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall & HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Note: Programs installed for all users are shown here.

| Name | Publisher | Installed On | Version |
| --- | --- | --- | --- |
| Microsoft Edge | Microsoft Corporation | 27/09/2020 | 84.0.522.52 |
| Microsoft Edge Update |  |  | 1.3.137.99 |

Table 2: [Registry] Installed Programs - System (Basic)

# [WMI] Operating System

This data is collected from the Win32\_OperatingSystem WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-operatingsystem

| Item | Value |
| --- | --- |
| Build Number | 19042 |
| Caption | Microsoft Windows 10 Enterprise |
| CS Name | WS-01 |
| Encryption Level | 256 |
| Install Date | 21/11/2020 16:16 |
| Operating System SKU | Enterprise Edition |
| OS Architecture | 64-bit |
| OS Product Suite | - Terminal Services is installed, but only one interactive session is supported. |
| Product Type | Workstation |
| Service Pack Major Version | 0 |
| Service Pack Minor Version | 0 |
| Total Visible Memory Size (GB) | 1.72 |
| Version | 10.0.19042 |

Table 3: [WMI] Operating System

# [WMI] Computer System

This data is collected from the Win32\_ComputerSystem WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-computersystem

| Item | Value |
| --- | --- |
| Admin Password Status | Unknown |
| Name | WS-01 |
| Domain | ad.gr303.co.uk |
| Domain Role | Member Workstation |
| Manufacturer | Microsoft Corporation |
| Model | Virtual Machine |
| Number Of Logical Processors | 1 |
| Part Of Domain | True |
| Roles | LM\_Workstation  LM\_Server  NT |
| System Type | x64-based PC |
| Total Physical Memory (GB) | 2 |
| Wake Up Type | Power Switch |

Table 4: [WMI] Computer System

# [WMI] Windows System Assessment Tool

This data is collected from the Win32\_WinSat WMI class. For more information please go to https://docs.microsoft.com/en-us/windows/win32/winsat/win32-winsat

| Item | Value |
| --- | --- |
| CPU Score | 0 |
| D3D Score | 0 |
| Disk Score | 0 |
| Graphics Score | 0 |
| Memory Score | 0 |
| Time Taken | MostRecentAssessment |
| WinSat Assessment State | No Assessement Available |
| Win SPR Level | 0 |

Table 5: [WMI] Windows System Assessment Tool

# [WMI] Network Adapter Configuration

This data is collected from the Win32\_NetworkAdapterConfiguration WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-networkadapterconfiguration

Note: There is a known bug in this method for collecting DHCP lease times for this Operating System. Times below marked between \*\*\* \*\*\* need to be validated using other means. For more information please go to https://social.technet.microsoft.com/Forums/windows/en-US/e22b8272-aafa-484b-a68f-1347c71381b0/wmi-cim-dhcp-information-wrong?forum=win10itprogeneral

| Item | Value |
| --- | --- |
| DHCP Lease Expires | \*\*\* \*\*\* |
| Description | Microsoft Hyper-V Network Adapter |
| DHCP Enabled | False |
| DHCP Lease Obtained | \*\*\* \*\*\* |
| DHCP Server |  |
| DNS Domain |  |
| DNS Domain Suffix Search Order | ad.gr303.co.uk |
| DNS Enabled For WINS Resolution | False |
| DNS Hostname | WS-01 |
| DNS Server Search Order | 10.0.0.1 |
| IP Address | 10.0.0.15 |
| IP Enabled | True |
| IP Filter Security Enabled | False |
| WINS Enable LMhosts Lookup | True |
| WINS Primary Server |  |
| WINS Secondary Server |  |
| Caption | [00000001] Microsoft Hyper-V Network Adapter |
| Default IP Gateway | 10.0.0.254 |
| IP Subnet | 255.0.0.0 |
| MAC Address | 00:15:5D:C8:B1:02 |

Table 6: [WMI] Network Adapter Configuration

# [WMI] Physical Memory

This data is collected from the Win32\_PhysicalMemory WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-physicalmemory

| Device Locator | Memory Type | Configured Clock Speed (MHz) | Capacity (GB) |
| --- | --- | --- | --- |
| M0001 | Unknown | 0 | 1 |

Table 7: [WMI] Physical Memory (Basic)

# [WMI] Processor

This data is collected from the Win32\_Processor WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-processor

| Item | Value |
| --- | --- |
| Address Width (Bits) | 64 |
| Caption | AMD64 Family 23 Model 24 Stepping 1 |
| CPU Status | CPU Enabled |
| Current Clock Speed (MHz) | 2096 |
| Data Width (Bits) | 64 |
| Device ID | CPU0 |
| Ext Clock (MHz) | 100 |
| L2 Cache Size (KB) |  |
| L2 Cache Speed (MHz) |  |
| L3 Cache Size (KB) | 0 |
| L3 Cache Speed (MHz) | 0 |
| Load Percentage | 3 |
| Manufacturer | AuthenticAMD |
| Max Clock Speed (MHz) | 2096 |
| Name | AMD Ryzen 5 PRO 3500U w/ Radeon Vega Mobile Gfx |
| Number Of Cores | 1 |
| Number Of Enabled Cores | 1 |
| Number Of Logical Processors | 1 |
| Part Number | None |
| Power Management Supported | False |
| Processor Type | Central Processor |
| Serial Number | None |
| Thread Count | 2 |
| VM Monitor Mode Extensions | False |
| Virtualization Firmware Enabled | True |

Table 8: [WMI] Processor

# [WMI] Logical Disk

This data is collected from the Win32\_LogicalDisk WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-logicaldisk

| Device ID | Volume Name | Type | Size (GB) | Free Space (GB) | Free (%) |
| --- | --- | --- | --- | --- | --- |
| C: |  | Local Disk | 29.39 | 10.9 | 37.1 |
| D: | CPBA\_X64FRE\_EN-GB\_DV9 | Compact Disc | 5.54 | 0 | 0 |

Table 9: [WMI] Logical Disk (Basic)

# [WMI] Disk Partition

This data is collected from the Win32\_DiskPartition WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-diskpartition

| Device ID | Bootable | Block Size (Bytes) | Disk Index | Primary Partition | Size (GB) |
| --- | --- | --- | --- | --- | --- |
| Disk #0, Partition #2 | False | 512 | 0 | False | 0.49 |
| Disk #0, Partition #1 | False | 512 | 0 | True | 29.39 |
| Disk #0, Partition #0 | True | 512 | 0 | True | 0.1 |

Table 10: [WMI] Disk Partition (Basic)

# [WMI] Share

This data is collected from the Win32\_Share WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-share

| Name | Caption | Description | Path | Type |
| --- | --- | --- | --- | --- |
| ADMIN$ | Remote Admin | Remote Admin | C:\Windows | Disk Drive Admin |
| C$ | Default share | Default share | C:\ | Disk Drive Admin |
| IPC$ | Remote IPC | Remote IPC |  | IPC Admin |

Table 11: [WMI] Share

# [WMI] Start Up Command

This data is collected from the Win32\_StartUpCommand WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-startupcommand

| Name | Command | User |
| --- | --- | --- |
| OneDrive | "C:\Users\GR\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background | WS-01\GR |
| OneDriveSetup | C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup | NT AUTHORITY\NETWORK SERVICE |
| OneDriveSetup | C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup | NT AUTHORITY\LOCAL SERVICE |
| SecurityHealth | %windir%\system32\SecurityHealthSystray.exe | Public |

Table 12: [WMI] Start Up Command (Basic)

# [WMI] Page File Usage

This data is collected from the Win32\_PageFileUsage WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-pagefileusage

| Item | Value |
| --- | --- |
| Current Usage (GB) | 0.08 |
| Allocated Base Size (GB) | 1.73 |
| Caption | C:\pagefile.sys |
| Description | C:\pagefile.sys |
| Name | C:\pagefile.sys |

Table 13: [WMI] Page File Usage

# [WMI] Quick Fix Engineering (Updates)

This data is collected from the Win32\_QuickFixEngineering WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-quickfixengineering

| Hot Fix ID | Description | Installed On |
| --- | --- | --- |
| KB4562830 | Update |  |
| KB4570334 | Security Update |  |
| KB4571756 | Update |  |
| KB4576478 | Update |  |
| KB4577266 | Security Update |  |

Table 14: [WMI] Quick Fix Engineering (Basic)

# [WMI] System Enclosure

This data is collected from the Win32\_SystemEnclosure WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-systemenclosure

| Item | Value |
| --- | --- |
| Chassis Types | Desktop |
| Lock Present | False |
| Manufacturer | Microsoft Corporation |
| Model |  |
| Security Status | Unknown |
| Serial Number | 0899-4214-6044-8627-8853-6053-55 |

Table 15: [WMI] System Enclosure

# [WMI] Boot Configuration

This data is collected from the Win32\_BootConfiguration WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-bootconfiguration

| Item | Value |
| --- | --- |
| Boot Directory | C:\Windows |
| Caption | \Device\Harddisk0\Partition1 |
| Configuration Path | C:\Windows |
| Description | \Device\Harddisk0\Partition1 |
| Scratch Directory | C:\Windows\system32\config\systemprofile\AppData\Local\Temp |

Table 16: [WMI] Boot Configuration

# [WMI] BIOS

This data is collected from the Win32\_Bios WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-bios

| Item | Value |
| --- | --- |
| BIOS Version | VRTUAL - 1 Hyper-V UEFI Release v4.0 Microsoft - 100032 |
| BIOS Characteristics | - BIOS Characteristics not supported  - Plug and Play is supported  - Boot from CD is supported  - Selectable Boot is supported  - EDD (Enhanced Disk Drive) Specification is supported  - Int 14h, Serial Services are supported  - ACPI supported  - 42 Reserved for BIOS vendor  - 43 Reserved for BIOS vendor  - 44 Reserved for BIOS vendor |
| Build Number |  |
| Caption | Hyper-V UEFI Release v4.0 |
| Description | Hyper-V UEFI Release v4.0 |
| Manufacturer | Microsoft Corporation |
| Name | Hyper-V UEFI Release v4.0 |
| Primary BIOS | True |
| Release Date | 30/01/2019 |
| SM BIOS Version | Hyper-V UEFI Release v4.0 |
| SM BIOS Major Version | 3 |
| SM BIOS Minor Version | 1 |
| SM BIOS Present | True |
| Serial Number | 0899-4214-6044-8627-8853-6053-55 |
| Software Element ID | Hyper-V UEFI Release v4.0 |
| Software Element State | Running |
| System BIOS Major Version | 4 |
| System BIOS Minor Version | 0 |
| Version | VRTUAL - 1 |

Table 17: [WMI] BIOS

# [WMI] User Accounts

This data is collected from the Win32\_UserAccounts WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-useraccount

| Domain | Name | Disabled | Password Expires | Password Required | Locked Out |
| --- | --- | --- | --- | --- | --- |
| WS-01 | Administrator | True | False | True | False |
| WS-01 | DefaultAccount | True | False | False | False |
| WS-01 | GR | False | False | False | False |
| WS-01 | Guest | True | False | False | False |
| WS-01 | WDAGUtilityAccount | True | True | True | False |

Table 18: [WMI] User Account (Basic)

# [WMI] Groups

This data is collected from the Win32\_Group WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-group

| Domain | Name | Local Group |
| --- | --- | --- |
| WS-01 | Access Control Assistance Operators | True |
| WS-01 | Administrators | True |
| WS-01 | Backup Operators | True |
| WS-01 | Cryptographic Operators | True |
| WS-01 | Device Owners | True |
| WS-01 | Distributed COM Users | True |
| WS-01 | Event Log Readers | True |
| WS-01 | Guests | True |
| WS-01 | Hyper-V Administrators | True |
| WS-01 | IIS\_IUSRS | True |
| WS-01 | Network Configuration Operators | True |
| WS-01 | Performance Log Users | True |
| WS-01 | Performance Monitor Users | True |
| WS-01 | Power Users | True |
| WS-01 | Remote Desktop Users | True |
| WS-01 | Remote Management Users | True |
| WS-01 | Replicator | True |
| WS-01 | System Managed Accounts Group | True |
| WS-01 | Users | True |

Table 19: [WMI] Group (Basic)

# [WMI] Group Membership

This data is collected from the Win32\_Group & Win32\_GroupUser WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-group & https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-groupuser

| Group | Members |
| --- | --- |

Table 20: [WMI] Group Membership

# [WMI] System Accounts

This data is collected from the Win32\_SystemAccount WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-systemaccount

| Domain | Name | Local Account |
| --- | --- | --- |
| WS-01 | ANONYMOUS LOGON | True |
| WS-01 | Authenticated Users | True |
| WS-01 | BATCH | True |
| WS-01 | BUILTIN | True |
| WS-01 | CREATOR GROUP | True |
| WS-01 | CREATOR GROUP SERVER | True |
| WS-01 | CREATOR OWNER | True |
| WS-01 | CREATOR OWNER SERVER | True |
| WS-01 | DIALUP | True |
| WS-01 | ENTERPRISE DOMAIN CONTROLLERS | True |
| WS-01 | Everyone | True |
| WS-01 | INTERACTIVE | True |
| WS-01 | IUSR | True |
| WS-01 | LOCAL | True |
| WS-01 | LOCAL SERVICE | True |
| WS-01 | NETWORK | True |
| WS-01 | NETWORK SERVICE | True |
| WS-01 | OWNER RIGHTS | True |
| WS-01 | PROXY | True |
| WS-01 | REMOTE INTERACTIVE LOGON | True |
| WS-01 | RESTRICTED | True |
| WS-01 | SELF | True |
| WS-01 | SERVICE | True |
| WS-01 | SYSTEM | True |
| WS-01 | TERMINAL SERVER USER | True |

Table 21: [WMI] System Account (Basic)

# [WMI] Time Zone

This data is collected from the Win32\_TimeZone WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-timezone

| Item | Value |
| --- | --- |
| Caption | (UTC+00:00) Dublin, Edinburgh, Lisbon, London |
| Standard Name | GMT Standard Time |

Table 22: [WMI] Time Zone

# [WMI] Registry

This data is collected from the Win32\_Registry WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-registry

| Item | Value |
| --- | --- |
| Current Size (MB) | 87 |
| Maximum Size (MB) | 4095 |

Table 23: [WMI] Registry

# [WMI] Environment

This data is collected from the Win32\_Environment WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-environment

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Name | ComSpec |
| System Variable | True |
| Caption | SYSTEM\ComSpec |
| User Name | SYSTEM |
| Variable Value | %SystemRoot%\system32\cmd.exe |
| ------ BLOCK 2 ------ | |
| Name | DriverData |
| System Variable | True |
| Caption | SYSTEM\DriverData |
| User Name | SYSTEM |
| Variable Value | C:\Windows\System32\Drivers\DriverData |
| ------ BLOCK 3 ------ | |
| Name | NUMBER\_OF\_PROCESSORS |
| System Variable | True |
| Caption | SYSTEM\NUMBER\_OF\_PROCESSORS |
| User Name | SYSTEM |
| Variable Value | 1 |
| ------ BLOCK 4 ------ | |
| Name | OneDrive |
| System Variable | False |
| Caption | WS-01\GR\OneDrive |
| User Name | WS-01\GR |
| Variable Value | C:\Users\GR\OneDrive |
| ------ BLOCK 5 ------ | |
| Name | OS |
| System Variable | True |
| Caption | SYSTEM\OS |
| User Name | SYSTEM |
| Variable Value | Windows\_NT |
| ------ BLOCK 6 ------ | |
| Name | Path |
| System Variable | False |
| Caption | NT AUTHORITY\LOCAL SERVICE\Path |
| User Name | NT AUTHORITY\LOCAL SERVICE |
| Variable Value | %USERPROFILE%\AppData\Local\Microsoft\WindowsApps |
| ------ BLOCK 7 ------ | |
| Name | Path |
| System Variable | True |
| Caption | SYSTEM\Path |
| User Name | SYSTEM |
| Variable Value | %SystemRoot%\system32  %SystemRoot%  %SystemRoot%\System32\Wbem  %SYSTEMROOT%\System32\WindowsPowerShell\v1.0\  %SYSTEMROOT%\System32\OpenSSH\ |
| ------ BLOCK 8 ------ | |
| Name | Path |
| System Variable | False |
| Caption | NT AUTHORITY\NETWORK SERVICE\Path |
| User Name | NT AUTHORITY\NETWORK SERVICE |
| Variable Value | %USERPROFILE%\AppData\Local\Microsoft\WindowsApps |
| ------ BLOCK 9 ------ | |
| Name | Path |
| System Variable | False |
| Caption | WS-01\GR\Path |
| User Name | WS-01\GR |
| Variable Value | %USERPROFILE%\AppData\Local\Microsoft\WindowsApps |
| ------ BLOCK 10 ------ | |
| Name | Path |
| System Variable | False |
| Caption | NT AUTHORITY\SYSTEM\Path |
| User Name | NT AUTHORITY\SYSTEM |
| Variable Value | %USERPROFILE%\AppData\Local\Microsoft\WindowsApps |
| ------ BLOCK 11 ------ | |
| Name | Path |
| System Variable | False |
| Caption | AD\Administrator\Path |
| User Name | AD\Administrator |
| Variable Value | %USERPROFILE%\AppData\Local\Microsoft\WindowsApps |
| ------ BLOCK 12 ------ | |
| Name | PATHEXT |
| System Variable | True |
| Caption | SYSTEM\PATHEXT |
| User Name | SYSTEM |
| Variable Value | .COM  .EXE  .BAT  .CMD  .VBS  .VBE  .JS  .JSE  .WSF  .WSH  .MSC |
| ------ BLOCK 13 ------ | |
| Name | PROCESSOR\_ARCHITECTURE |
| System Variable | True |
| Caption | SYSTEM\PROCESSOR\_ARCHITECTURE |
| User Name | SYSTEM |
| Variable Value | AMD64 |
| ------ BLOCK 14 ------ | |
| Name | PROCESSOR\_IDENTIFIER |
| System Variable | True |
| Caption | SYSTEM\PROCESSOR\_IDENTIFIER |
| User Name | SYSTEM |
| Variable Value | AMD64 Family 23 Model 24 Stepping 1, AuthenticAMD |
| ------ BLOCK 15 ------ | |
| Name | PROCESSOR\_LEVEL |
| System Variable | True |
| Caption | SYSTEM\PROCESSOR\_LEVEL |
| User Name | SYSTEM |
| Variable Value | 23 |
| ------ BLOCK 16 ------ | |
| Name | PROCESSOR\_REVISION |
| System Variable | True |
| Caption | SYSTEM\PROCESSOR\_REVISION |
| User Name | SYSTEM |
| Variable Value | 1801 |
| ------ BLOCK 17 ------ | |
| Name | PSModulePath |
| System Variable | True |
| Caption | SYSTEM\PSModulePath |
| User Name | SYSTEM |
| Variable Value | %ProgramFiles%\WindowsPowerShell\Modules  %SystemRoot%\system32\WindowsPowerShell\v1.0\Modules |
| ------ BLOCK 18 ------ | |
| Name | TEMP |
| System Variable | True |
| Caption | SYSTEM\TEMP |
| User Name | SYSTEM |
| Variable Value | %SystemRoot%\TEMP |
| ------ BLOCK 19 ------ | |
| Name | TEMP |
| System Variable | False |
| Caption | NT AUTHORITY\NETWORK SERVICE\TEMP |
| User Name | NT AUTHORITY\NETWORK SERVICE |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 20 ------ | |
| Name | TEMP |
| System Variable | False |
| Caption | WS-01\GR\TEMP |
| User Name | WS-01\GR |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 21 ------ | |
| Name | TEMP |
| System Variable | False |
| Caption | AD\Administrator\TEMP |
| User Name | AD\Administrator |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 22 ------ | |
| Name | TEMP |
| System Variable | False |
| Caption | NT AUTHORITY\SYSTEM\TEMP |
| User Name | NT AUTHORITY\SYSTEM |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 23 ------ | |
| Name | TEMP |
| System Variable | False |
| Caption | NT AUTHORITY\LOCAL SERVICE\TEMP |
| User Name | NT AUTHORITY\LOCAL SERVICE |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 24 ------ | |
| Name | TMP |
| System Variable | False |
| Caption | AD\Administrator\TMP |
| User Name | AD\Administrator |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 25 ------ | |
| Name | TMP |
| System Variable | False |
| Caption | WS-01\GR\TMP |
| User Name | WS-01\GR |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 26 ------ | |
| Name | TMP |
| System Variable | False |
| Caption | NT AUTHORITY\SYSTEM\TMP |
| User Name | NT AUTHORITY\SYSTEM |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 27 ------ | |
| Name | TMP |
| System Variable | False |
| Caption | NT AUTHORITY\LOCAL SERVICE\TMP |
| User Name | NT AUTHORITY\LOCAL SERVICE |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 28 ------ | |
| Name | TMP |
| System Variable | False |
| Caption | NT AUTHORITY\NETWORK SERVICE\TMP |
| User Name | NT AUTHORITY\NETWORK SERVICE |
| Variable Value | %USERPROFILE%\AppData\Local\Temp |
| ------ BLOCK 29 ------ | |
| Name | TMP |
| System Variable | True |
| Caption | SYSTEM\TMP |
| User Name | SYSTEM |
| Variable Value | %SystemRoot%\TEMP |
| ------ BLOCK 30 ------ | |
| Name | USERNAME |
| System Variable | True |
| Caption | SYSTEM\USERNAME |
| User Name | SYSTEM |
| Variable Value | SYSTEM |
| ------ BLOCK 31 ------ | |
| Name | windir |
| System Variable | True |
| Caption | SYSTEM\windir |
| User Name | SYSTEM |
| Variable Value | %SystemRoot% |

Table 24: [WMI] Environment

# [WMI] CD ROM Drive

This data is collected from the Win32\_CDROMDrive WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-cdromdrive

| Item | Value |
| --- | --- |
| Availability | Running/Full Power |
| Capability Descriptions | Random Access  Supports Removable Media |
| Description | CD-ROM Drive |
| Device ID | SCSI\CDROM&VEN\_MSFT&PROD\_VIRTUAL\_DVD-ROM\5&2C54316E&0&000001 |
| Drive | D: |
| Manufacturer | (Standard CD-ROM drives) |
| Media Type | DVD-ROM |
| Name | Microsoft Virtual DVD-ROM |
| PNP Device ID | SCSI\CDROM&VEN\_MSFT&PROD\_VIRTUAL\_DVD-ROM\5&2C54316E&0&000001 |
| Serial Number |  |

Table 25: [WMI] CD ROM Drive

# [WMI] Video Controller

This data is collected from the Win32\_VideoController WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-videocontroller

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Adapter Compatibility | Microsoft |
| Adapter DAC Type |  |
| Adapter RAM (GB) | 0 |
| Availability | Running/Full Power |
| Device ID | VideoController1 |
| Driver Date | 21/06/2006 |
| Driver Version | 10.0.19041.1 |
| INF File Name | wvmbusvideo.inf |
| INF Section | HyperVideo\_Install |
| Installed Display Drivers |  |
| Name | Microsoft Hyper-V Video |
| PNP Device ID | VMBUS\{DA0A7802-E377-4AAC-8E77-0558EB1073F8}\{5620E0C7-8062-4DCE-AEB7-520C7EF76171} |
| Video Mode Description | 1024 x 768 x 4294967296 colors |
| Video Processor |  |
| ------ BLOCK 2 ------ | |
| Adapter Compatibility | Microsoft |
| Adapter DAC Type |  |
| Adapter RAM (GB) | 0 |
| Availability | Running/Full Power |
| Device ID | VideoController2 |
| Driver Date | 21/06/2006 |
| Driver Version | 10.0.19041.423 |
| INF File Name | rdpidd.inf |
| INF Section | RdpIdd\_Install.NT |
| Installed Display Drivers |  |
| Name | Microsoft Remote Display Adapter |
| PNP Device ID | SWD\REMOTEDISPLAYENUM\RDPIDD\_INDIRECTDISPLAY&SESSIONID\_0002 |
| Video Mode Description | 1200 x 900 x 4294967296 colors |
| Video Processor |  |

Table 26: [WMI] Video Controller

# [WMI] Sound Device

This data is collected from the Win32\_SoundDevice WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-sounddevice

| Item | Value |
| --- | --- |
| No sound devices installed | |

Table 27: [WMI] Sound Device

# [WMI] Printers

This data is collected from the Win32\_Printer WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-printer

| Name | Local | Network | Shared |
| --- | --- | --- | --- |
| Fax | True | False | False |
| Microsoft Print to PDF | True | False | False |
| Microsoft XPS Document Writer | True | False | False |

Table 28: [WMI] Printer (Basic)

# [WMI] Disk Drive

This data is collected from the Win32\_DiskDrive WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-diskdrive

| Item | Value |
| --- | --- |
| Caption | Microsoft Virtual Disk |
| Firmware Revision | 1.0 |
| Interface Type | SCSI |
| Manufacturer | (Standard disk drives) |
| Model | Microsoft Virtual Disk |
| Name | \\.\PHYSICALDRIVE0 |
| PNP Device ID | SCSI\DISK&VEN\_MSFT&PROD\_VIRTUAL\_DISK\5&2C54316E&0&000000 |
| Partitions | 3 |
| Serial Number |  |
| Size (GB) | 30 |

Table 29: [WMI] Disk Drive

# [WMI] Encryptable Volume

This data is collected from the Win32\_EncryptableVolume WMI class. For more information please go to https://docs.microsoft.com/en-us/windows/win32/secprov/win32-encryptablevolume

| Item | Value |
| --- | --- |
| Drive Letter | C: |
| Conversion Status | Fully Decrypted |
| Encryption Method | None |
| Initialized For Protection | False |
| Protection Status | Protection Off |
| Volume Type | OS Volume |

Table 30: [WMI] Encryption Status

# [WMI] Firewall Product

This data is collected from the FirewallProduct WMI class. There is no Microsoft published information on this class.

| Item | Value |
| --- | --- |
| No firewall product installed | |

Table 31: [WMI] Firewall Product

# [WMI] Antivirus Product

This data is collected from the AntivirusProduct WMI class. There is no Microsoft published information on this class.

| Item | Value |
| --- | --- |
| Display Name | Windows Defender |
| Product EXE | windowsdefender:// |
| Reporting EXE | %ProgramFiles%\Windows Defender\MsMpeng.exe |
| Timestamp | Sat, 21 Nov 2020 16:58:05 GMT |

Table 32: [WMI] Antivirus Product

# [WMI] Antispyware Product

This data is collected from the AntisypwareProduct WMI class. There is no Microsoft published information on this class.

| Item | Value |
| --- | --- |
| No antispyware products installed | |

Table 33: [WMI] Antispyware Product

# [WMI] Optional Features

This data is collected from the Win32\_OptionalFeature WMI class. For more information please go to https://docs.microsoft.com/en-gb/windows/desktop/CIMWin32Prov/win32-optionalfeature

| Caption | Name |
| --- | --- |
| Internet Explorer 11 | Internet-Explorer-Optional-amd64 |
| Media Features | MediaPlayback |
| Windows PowerShell 2.0 Engine | MicrosoftWindowsPowerShellV2 |
| Windows PowerShell 2.0 | MicrosoftWindowsPowerShellV2Root |
| Remote Differential Compression API Support | MSRDC-Infrastructure |
| .NET Framework 4.8 Advanced Services | NetFx4-AdvSrvs |
| Print and Document Services | Printing-Foundation-Features |
| Internet Printing Client | Printing-Foundation-InternetPrinting-Client |
| Microsoft Print to PDF | Printing-PrintToPDFServices-Features |
| Microsoft XPS Document Writer | Printing-XPSServices-Features |
| Windows Search | SearchEngine-Client-Package |
| SMB Direct | SmbDirect |
| WCF Services | WCF-Services45 |
| TCP Port Sharing | WCF-TCP-PortSharing45 |
|  | Windows-Defender-Default-Definitions |
| Windows Media Player | WindowsMediaPlayer |
| Work Folders Client | WorkFolders-Client |

Table 34: [WMI] Optional Features

# [System] Computer Certificates

This data is collected from the System.Security.Cryptography.X509Certificates.X509Store. For more information please go to https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.x509certificates.x509store?view=net-5.0

| Store | Subject | Issuer | Valid From | Expiration |
| --- | --- | --- | --- | --- |
| AuthRoot | DigiCert Global Root G2 | DigiCert Global Root G2 | 01/08/2013 13:00:00 | 15/01/2038 12:00:00 |
| AuthRoot | Baltimore CyberTrust Root | Baltimore CyberTrust Root | 12/05/2000 19:46:00 | 13/05/2025 00:59:00 |
| AuthRoot | DigiCert Global Root CA | DigiCert Global Root CA | 10/11/2006 00:00:00 | 10/11/2031 00:00:00 |
| AuthRoot | Class 3 Public Primary Certification Authority | Class 3 Public Primary Certification Authority | 29/01/1996 00:00:00 | 02/08/2028 00:59:59 |
| AuthRoot | Hotspot 2.0 Trust Root CA - 03 | Hotspot 2.0 Trust Root CA - 03 | 08/12/2013 12:00:00 | 08/12/2043 12:00:00 |
| AuthRoot | Class 3 Public Primary Certification Authority | Class 3 Public Primary Certification Authority | 29/01/1996 00:00:00 | 07/01/2004 23:59:59 |
| CA | Root Agency | Root Agency | 28/05/1996 23:02:59 | 31/12/2039 23:59:59 |
| CA | www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign | Class 3 Public Primary Certification Authority | 17/04/1997 01:00:00 | 25/10/2016 00:59:59 |
| CA | Microsoft Windows Hardware Compatibility | Microsoft Root Authority | 01/10/1997 08:00:00 | 31/12/2002 07:00:00 |
| eSIM Certification Authorities | GSM Association - RSP2 Root CI1 | GSM Association - RSP2 Root CI1 | 22/02/2017 00:00:00 | 21/02/2052 23:59:59 |
| eSIM Certification Authorities | CMCA eSIM Root CA\_NIST | CMCA eSIM Root CA\_NIST | 05/09/2017 03:00:00 | 05/09/2052 03:00:00 |
| eSIM Certification Authorities | China Unicom eSIM Root CA | China Unicom eSIM Root CA | 06/03/2017 17:00:00 | 06/03/2037 17:00:00 |
| FlightRoot | Microsoft Development Root Certificate Authority 2014 | Microsoft Development Root Certificate Authority 2014 | 28/05/2014 17:43:46 | 28/05/2039 17:51:48 |
| FlightRoot | Microsoft ECC Development Root Certificate Authority 2018 | Microsoft ECC Development Root Certificate Authority 2018 | 27/02/2018 20:30:58 | 27/02/2043 20:38:56 |
| Remote Desktop | WS-01.ad.gr303.co.uk | WS-01.ad.gr303.co.uk | 20/11/2020 16:55:59 | 22/05/2021 17:55:59 |
| ROOT | Microsoft Root Certificate Authority | Microsoft Root Certificate Authority | 10/05/2001 00:19:22 | 10/05/2021 00:28:13 |
| ROOT | Thawte Timestamping CA | Thawte Timestamping CA | 01/01/1997 00:00:00 | 31/12/2020 23:59:59 |
| ROOT | Microsoft Root Authority | Microsoft Root Authority | 10/01/1997 07:00:00 | 31/12/2020 07:00:00 |
| ROOT | Symantec Enterprise Mobile Root for Microsoft | Symantec Enterprise Mobile Root for Microsoft | 15/03/2012 00:00:00 | 14/03/2032 23:59:59 |
| ROOT | Microsoft Root Certificate Authority 2011 | Microsoft Root Certificate Authority 2011 | 22/03/2011 22:05:28 | 22/03/2036 22:13:04 |
| ROOT | Microsoft Authenticode(tm) Root Authority | Microsoft Authenticode(tm) Root Authority | 01/01/1995 08:00:01 | 31/12/1999 23:59:59 |
| ROOT | Microsoft Root Certificate Authority 2010 | Microsoft Root Certificate Authority 2010 | 23/06/2010 22:57:24 | 23/06/2035 23:04:01 |
| ROOT | Microsoft ECC TS Root Certificate Authority 2018 | Microsoft ECC TS Root Certificate Authority 2018 | 27/02/2018 20:51:34 | 27/02/2043 21:00:12 |
| ROOT | Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 13/05/1997 17:12:59 | 30/12/1999 23:59:59 |
| ROOT | NO LIABILITY ACCEPTED | NO LIABILITY ACCEPTED | 12/05/1997 01:00:00 | 07/01/2004 23:59:59 |
| ROOT | Microsoft ECC Product Root Certificate Authority 2018 | Microsoft ECC Product Root Certificate Authority 2018 | 27/02/2018 20:42:08 | 27/02/2043 20:50:46 |
| ROOT | Microsoft Time Stamp Root Certificate Authority 2014 | Microsoft Time Stamp Root Certificate Authority 2014 | 22/10/2014 23:08:57 | 22/10/2039 23:15:19 |
| ROOT | DigiCert Global Root G2 | DigiCert Global Root G2 | 01/08/2013 13:00:00 | 15/01/2038 12:00:00 |
| ROOT | Baltimore CyberTrust Root | Baltimore CyberTrust Root | 12/05/2000 19:46:00 | 13/05/2025 00:59:00 |
| ROOT | DigiCert Global Root CA | DigiCert Global Root CA | 10/11/2006 00:00:00 | 10/11/2031 00:00:00 |
| ROOT | Class 3 Public Primary Certification Authority | Class 3 Public Primary Certification Authority | 29/01/1996 00:00:00 | 02/08/2028 00:59:59 |
| ROOT | Hotspot 2.0 Trust Root CA - 03 | Hotspot 2.0 Trust Root CA - 03 | 08/12/2013 12:00:00 | 08/12/2043 12:00:00 |
| ROOT | Class 3 Public Primary Certification Authority | Class 3 Public Primary Certification Authority | 29/01/1996 00:00:00 | 07/01/2004 23:59:59 |
| TestSignRoot | Microsoft ECC Testing Root Certificate Authority 2017 | Microsoft ECC Testing Root Certificate Authority 2017 | 09/11/2017 19:53:14 | 09/11/2042 20:01:55 |
| TestSignRoot | Microsoft Testing Root Certificate Authority 2010 | Microsoft Testing Root Certificate Authority 2010 | 17/06/2010 21:58:02 | 17/06/2035 22:04:11 |
| TestSignRoot | Microsoft Test Root Authority | Microsoft Test Root Authority | 10/01/1999 07:00:00 | 31/12/2020 07:00:00 |
| TrustedAppRoot | Microsoft VSMC PCA 2017 | Microsoft Mobile Root Certificate Authority 2015 | 26/09/2017 19:56:47 | 26/09/2032 20:06:47 |
| Windows Live ID Token Issuer | Token Signing Public Key | Token Signing Public Key | 09/05/2016 21:40:55 | 08/05/2021 21:40:55 |
| Windows Live ID Token Issuer | Token Signing Public Key | Token Signing Public Key | 02/07/2013 22:10:37 | 01/07/2018 22:10:37 |

Table 35: [System] Computer Certificates (Basic)