Build Report for WS-01

**Report type:** Detailed

**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

Basic 5

Detailed 5

[WMI] Operating System 6

[WMI] Computer System 7

[WMI] Windows System Assessment Tool 8

[WMI] Network Adapter Configuration 9

[WMI] Physical Memory 10

Basic 10

Detailed 10

[WMI] Processor 11

[WMI] Logical Disk 12

Basic 12

Detailed 12

[WMI] Disk Partition 13

Basic 13

Detailed 13

[WMI] Share 15

[WMI] Start Up Command 16

Basic 16

Detailed 16

[WMI] Page File Usage 18

[WMI] Quick Fix Engineering (Updates) 19

Basic 19

Detailed 19

[WMI] System Enclosure 21

[WMI] Boot Configuration 22

[WMI] BIOS 23

[WMI] User Accounts 24

Basic 24

Detailed 24

[WMI] Groups 27

Basic 27

Detailed 27

[WMI] Group Membership 32

[WMI] System Accounts 33

Basic 33

Detailed 33

[WMI] Time Zone 39

[WMI] Registry 40

[WMI] Environment 41

[WMI] CD ROM Drive 46

[WMI] Video Controller 47

[WMI] Sound Device 48

[WMI] Printers 49

Basic 49

Detailed 49

[WMI] Disk Drive 51

[WMI] Encryptable Volume 52

[WMI] Firewall Product 53

[WMI] Antivirus Product 54

[WMI] Antispyware Product 55

[WMI] Optional Features 56

[WMI] Services 58

[WMI] Processes 65

[WMI] System Drivers 68

[WMI] PNP Entities 78

[System] Computer Certificates 88

Basic 88

Detailed 90

# [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.

## Basic

| 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)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Source | System |
| Name | Microsoft Edge |
| Version | 84.0.522.52 |
| Location | C:\Program Files (x86)\Microsoft\Edge\Application |
| Publisher | Microsoft Corporation |
| Install date |  |
| Architecture | x64 |
| Comments |  |
| ------ BLOCK 2 ------ | |
| Source | System |
| Name | Microsoft Edge Update |
| Version | 1.3.137.99 |
| Location |  |
| Publisher |  |
| Install date |  |
| Architecture | x64 |
| Comments |  |

Table 3: [Registry] Installed Program - System (Detailed)

# [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 4: [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 5: [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 6: [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 7: [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

## Basic

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

Table 8: [WMI] Physical Memory (Basic)

## Detailed

| Item | Value |
| --- | --- |
| Capacity (GB) | 1 |
| Configured Clock Speed (MHz) | 0 |
| Data Width (Bits) |  |
| Device Locator | M0001 |
| Form Factor | Unknown |
| Manufacturer | Microsoft Corporation |
| Memory Type | Unknown |
| Model |  |
| Part Number | None |
| Serial Number | None |
| Speed (Nanoseconds) |  |

Table 9: [WMI] Physical Memory (Detailed)

# [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 10: [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

## Basic

| 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 11: [WMI] Logical Disk (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Device ID | C: |
| Description | Local Fixed Disk |
| Drive Type | Local Disk |
| File System | NTFS |
| Free Space (GB) | 10.9 |
| Media Type | Fixed hard disk media |
| Size (GB) | 29.39 |
| Volume Name |  |
| Volume Serial Number | DE08F9A3 |
| ------ BLOCK 2 ------ | |
| Device ID | D: |
| Description | CD-ROM Disc |
| Drive Type | Compact Disc |
| File System | UDF |
| Free Space (GB) | 0 |
| Media Type | Removable media other than floppy |
| Size (GB) | 5.54 |
| Volume Name | CPBA\_X64FRE\_EN-GB\_DV9 |
| Volume Serial Number | D1B13C65 |

Table 12: [WMI] Logical Disk (Detailed)

# [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

## Basic

| 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 13: [WMI] Disk Partition (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Block Size (Bytes) | 512 |
| Bootable | False |
| Boot Partition | False |
| Description | GPT: Unknown |
| Device ID | Disk #0, Partition #2 |
| Disk Index | 0 |
| Number Of Blocks | 1034240 |
| Primary Partition | False |
| Size (GB) | 0.49 |
| ------ BLOCK 2 ------ | |
| Block Size (Bytes) | 512 |
| Bootable | False |
| Boot Partition | False |
| Description | GPT: Basic Data |
| Device ID | Disk #0, Partition #1 |
| Disk Index | 0 |
| Number Of Blocks | 61635657 |
| Primary Partition | True |
| Size (GB) | 29.39 |
| ------ BLOCK 3 ------ | |
| Block Size (Bytes) | 512 |
| Bootable | True |
| Boot Partition | True |
| Description | GPT: System |
| Device ID | Disk #0, Partition #0 |
| Disk Index | 0 |
| Number Of Blocks | 204800 |
| Primary Partition | True |
| Size (GB) | 0.1 |

Table 14: [WMI] Disk Partition (Detailed)

# [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 15: [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

## Basic

| 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 16: [WMI] Start Up Command (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Caption | OneDrive |
| Command | "C:\Users\GR\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background |
| Description | OneDrive |
| Name | OneDrive |
| User | WS-01\GR |
| ------ BLOCK 2 ------ | |
| Caption | OneDriveSetup |
| Command | C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup |
| Description | OneDriveSetup |
| Name | OneDriveSetup |
| User | NT AUTHORITY\NETWORK SERVICE |
| ------ BLOCK 3 ------ | |
| Caption | OneDriveSetup |
| Command | C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup |
| Description | OneDriveSetup |
| Name | OneDriveSetup |
| User | NT AUTHORITY\LOCAL SERVICE |
| ------ BLOCK 4 ------ | |
| Caption | SecurityHealth |
| Command | %windir%\system32\SecurityHealthSystray.exe |
| Description | SecurityHealth |
| Name | SecurityHealth |
| User | Public |

Table 17: [WMI] Start Up Command (Detailed)

# [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 18: [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

## Basic

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

Table 19: [WMI] Quick Fix Engineering (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Caption | http://support.microsoft.com/?kbid=4562830 |
| Description | Update |
| Hot Fix ID | KB4562830 |
| Installed By |  |
| Installed On |  |
| ------ BLOCK 2 ------ | |
| Caption | http://support.microsoft.com/?kbid=4570334 |
| Description | Security Update |
| Hot Fix ID | KB4570334 |
| Installed By |  |
| Installed On |  |
| ------ BLOCK 3 ------ | |
| Caption | https://support.microsoft.com/help/4571756 |
| Description | Update |
| Hot Fix ID | KB4571756 |
| Installed By |  |
| Installed On |  |
| ------ BLOCK 4 ------ | |
| Caption | http://support.microsoft.com/?kbid=4576478 |
| Description | Update |
| Hot Fix ID | KB4576478 |
| Installed By |  |
| Installed On |  |
| ------ BLOCK 5 ------ | |
| Caption | https://support.microsoft.com/help/4577266 |
| Description | Security Update |
| Hot Fix ID | KB4577266 |
| Installed By |  |
| Installed On |  |

Table 20: [WMI] Quick Fix Engineering (Detailed)

# [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 21: [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 22: [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 23: [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

## Basic

| 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 24: [WMI] User Account (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Account Type | Normal account |
| Caption | WS-01\Administrator |
| Description | Built-in account for administering the computer/domain |
| Disabled | True |
| Domain | WS-01 |
| Fullname |  |
| Local Account | True |
| Locked Out | False |
| Name | Administrator |
| Password Changeable | True |
| Password Expires | False |
| Password Required | True |
| SID | S-1-5-21-2505210889-1497311358-3084750444-500 |
| SID Type | User |
| ------ BLOCK 2 ------ | |
| Account Type | Normal account |
| Caption | WS-01\DefaultAccount |
| Description | A user account managed by the system. |
| Disabled | True |
| Domain | WS-01 |
| Fullname |  |
| Local Account | True |
| Locked Out | False |
| Name | DefaultAccount |
| Password Changeable | True |
| Password Expires | False |
| Password Required | False |
| SID | S-1-5-21-2505210889-1497311358-3084750444-503 |
| SID Type | User |
| ------ BLOCK 3 ------ | |
| Account Type | Normal account |
| Caption | WS-01\GR |
| Description |  |
| Disabled | False |
| Domain | WS-01 |
| Fullname |  |
| Local Account | True |
| Locked Out | False |
| Name | GR |
| Password Changeable | True |
| Password Expires | False |
| Password Required | False |
| SID | S-1-5-21-2505210889-1497311358-3084750444-1001 |
| SID Type | User |
| ------ BLOCK 4 ------ | |
| Account Type | Normal account |
| Caption | WS-01\Guest |
| Description | Built-in account for guest access to the computer/domain |
| Disabled | True |
| Domain | WS-01 |
| Fullname |  |
| Local Account | True |
| Locked Out | False |
| Name | Guest |
| Password Changeable | False |
| Password Expires | False |
| Password Required | False |
| SID | S-1-5-21-2505210889-1497311358-3084750444-501 |
| SID Type | User |
| ------ BLOCK 5 ------ | |
| Account Type | Normal account |
| Caption | WS-01\WDAGUtilityAccount |
| Description | A user account managed and used by the system for Windows Defender Application Guard scenarios. |
| Disabled | True |
| Domain | WS-01 |
| Fullname |  |
| Local Account | True |
| Locked Out | False |
| Name | WDAGUtilityAccount |
| Password Changeable | True |
| Password Expires | True |
| Password Required | True |
| SID | S-1-5-21-2505210889-1497311358-3084750444-504 |
| SID Type | User |

Table 25: [WMI] User Account (Detailed)

# [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

## Basic

| 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 26: [WMI] Group (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Caption | WS-01\Access Control Assistance Operators |
| Description | Members of this group can remotely query authorization attributes and permissions for resources on this computer. |
| Domain | WS-01 |
| Local Group | True |
| Name | Access Control Assistance Operators |
| SID | S-1-5-32-579 |
| SID Type | Alias |
| ------ BLOCK 2 ------ | |
| Caption | WS-01\Administrators |
| Description | Administrators have complete and unrestricted access to the computer/domain |
| Domain | WS-01 |
| Local Group | True |
| Name | Administrators |
| SID | S-1-5-32-544 |
| SID Type | Alias |
| ------ BLOCK 3 ------ | |
| Caption | WS-01\Backup Operators |
| Description | Backup Operators can override security restrictions for the sole purpose of backing up or restoring files |
| Domain | WS-01 |
| Local Group | True |
| Name | Backup Operators |
| SID | S-1-5-32-551 |
| SID Type | Alias |
| ------ BLOCK 4 ------ | |
| Caption | WS-01\Cryptographic Operators |
| Description | Members are authorized to perform cryptographic operations. |
| Domain | WS-01 |
| Local Group | True |
| Name | Cryptographic Operators |
| SID | S-1-5-32-569 |
| SID Type | Alias |
| ------ BLOCK 5 ------ | |
| Caption | WS-01\Device Owners |
| Description | Members of this group can change system-wide settings. |
| Domain | WS-01 |
| Local Group | True |
| Name | Device Owners |
| SID | S-1-5-32-583 |
| SID Type | Alias |
| ------ BLOCK 6 ------ | |
| Caption | WS-01\Distributed COM Users |
| Description | Members are allowed to launch, activate and use Distributed COM objects on this machine. |
| Domain | WS-01 |
| Local Group | True |
| Name | Distributed COM Users |
| SID | S-1-5-32-562 |
| SID Type | Alias |
| ------ BLOCK 7 ------ | |
| Caption | WS-01\Event Log Readers |
| Description | Members of this group can read event logs from local machine |
| Domain | WS-01 |
| Local Group | True |
| Name | Event Log Readers |
| SID | S-1-5-32-573 |
| SID Type | Alias |
| ------ BLOCK 8 ------ | |
| Caption | WS-01\Guests |
| Description | Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted |
| Domain | WS-01 |
| Local Group | True |
| Name | Guests |
| SID | S-1-5-32-546 |
| SID Type | Alias |
| ------ BLOCK 9 ------ | |
| Caption | WS-01\Hyper-V Administrators |
| Description | Members of this group have complete and unrestricted access to all features of Hyper-V. |
| Domain | WS-01 |
| Local Group | True |
| Name | Hyper-V Administrators |
| SID | S-1-5-32-578 |
| SID Type | Alias |
| ------ BLOCK 10 ------ | |
| Caption | WS-01\IIS\_IUSRS |
| Description | Built-in group used by Internet Information Services. |
| Domain | WS-01 |
| Local Group | True |
| Name | IIS\_IUSRS |
| SID | S-1-5-32-568 |
| SID Type | Alias |
| ------ BLOCK 11 ------ | |
| Caption | WS-01\Network Configuration Operators |
| Description | Members in this group can have some administrative privileges to manage configuration of networking features |
| Domain | WS-01 |
| Local Group | True |
| Name | Network Configuration Operators |
| SID | S-1-5-32-556 |
| SID Type | Alias |
| ------ BLOCK 12 ------ | |
| Caption | WS-01\Performance Log Users |
| Description | Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer |
| Domain | WS-01 |
| Local Group | True |
| Name | Performance Log Users |
| SID | S-1-5-32-559 |
| SID Type | Alias |
| ------ BLOCK 13 ------ | |
| Caption | WS-01\Performance Monitor Users |
| Description | Members of this group can access performance counter data locally and remotely |
| Domain | WS-01 |
| Local Group | True |
| Name | Performance Monitor Users |
| SID | S-1-5-32-558 |
| SID Type | Alias |
| ------ BLOCK 14 ------ | |
| Caption | WS-01\Power Users |
| Description | Power Users are included for backwards compatibility and possess limited administrative powers |
| Domain | WS-01 |
| Local Group | True |
| Name | Power Users |
| SID | S-1-5-32-547 |
| SID Type | Alias |
| ------ BLOCK 15 ------ | |
| Caption | WS-01\Remote Desktop Users |
| Description | Members in this group are granted the right to logon remotely |
| Domain | WS-01 |
| Local Group | True |
| Name | Remote Desktop Users |
| SID | S-1-5-32-555 |
| SID Type | Alias |
| ------ BLOCK 16 ------ | |
| Caption | WS-01\Remote Management Users |
| Description | Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user. |
| Domain | WS-01 |
| Local Group | True |
| Name | Remote Management Users |
| SID | S-1-5-32-580 |
| SID Type | Alias |
| ------ BLOCK 17 ------ | |
| Caption | WS-01\Replicator |
| Description | Supports file replication in a domain |
| Domain | WS-01 |
| Local Group | True |
| Name | Replicator |
| SID | S-1-5-32-552 |
| SID Type | Alias |
| ------ BLOCK 18 ------ | |
| Caption | WS-01\System Managed Accounts Group |
| Description | Members of this group are managed by the system. |
| Domain | WS-01 |
| Local Group | True |
| Name | System Managed Accounts Group |
| SID | S-1-5-32-581 |
| SID Type | Alias |
| ------ BLOCK 19 ------ | |
| Caption | WS-01\Users |
| Description | Users are prevented from making accidental or intentional system-wide changes and can run most applications |
| Domain | WS-01 |
| Local Group | True |
| Name | Users |
| SID | S-1-5-32-545 |
| SID Type | Alias |

Table 27: [WMI] Group (Detailed)

# [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 28: [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

## Basic

| 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 29: [WMI] System Account (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Caption | WS-01\ANONYMOUS LOGON |
| Description | WS-01\ANONYMOUS LOGON |
| Domain | WS-01 |
| Local Account | True |
| Name | ANONYMOUS LOGON |
| SID | S-1-5-7 |
| SID Type | Well Known Group |
| ------ BLOCK 2 ------ | |
| Caption | WS-01\Authenticated Users |
| Description | WS-01\Authenticated Users |
| Domain | WS-01 |
| Local Account | True |
| Name | Authenticated Users |
| SID | S-1-5-11 |
| SID Type | Well Known Group |
| ------ BLOCK 3 ------ | |
| Caption | WS-01\BATCH |
| Description | WS-01\BATCH |
| Domain | WS-01 |
| Local Account | True |
| Name | BATCH |
| SID | S-1-5-3 |
| SID Type | Well Known Group |
| ------ BLOCK 4 ------ | |
| Caption | WS-01\BUILTIN |
| Description | WS-01\BUILTIN |
| Domain | WS-01 |
| Local Account | True |
| Name | BUILTIN |
| SID | S-1-5-32 |
| SID Type | Domain |
| ------ BLOCK 5 ------ | |
| Caption | WS-01\CREATOR GROUP |
| Description | WS-01\CREATOR GROUP |
| Domain | WS-01 |
| Local Account | True |
| Name | CREATOR GROUP |
| SID | S-1-3-1 |
| SID Type | Well Known Group |
| ------ BLOCK 6 ------ | |
| Caption | WS-01\CREATOR GROUP SERVER |
| Description | WS-01\CREATOR GROUP SERVER |
| Domain | WS-01 |
| Local Account | True |
| Name | CREATOR GROUP SERVER |
| SID | S-1-3-3 |
| SID Type | Well Known Group |
| ------ BLOCK 7 ------ | |
| Caption | WS-01\CREATOR OWNER |
| Description | WS-01\CREATOR OWNER |
| Domain | WS-01 |
| Local Account | True |
| Name | CREATOR OWNER |
| SID | S-1-3-0 |
| SID Type | Well Known Group |
| ------ BLOCK 8 ------ | |
| Caption | WS-01\CREATOR OWNER SERVER |
| Description | WS-01\CREATOR OWNER SERVER |
| Domain | WS-01 |
| Local Account | True |
| Name | CREATOR OWNER SERVER |
| SID | S-1-3-2 |
| SID Type | Well Known Group |
| ------ BLOCK 9 ------ | |
| Caption | WS-01\DIALUP |
| Description | WS-01\DIALUP |
| Domain | WS-01 |
| Local Account | True |
| Name | DIALUP |
| SID | S-1-5-1 |
| SID Type | Well Known Group |
| ------ BLOCK 10 ------ | |
| Caption | WS-01\ENTERPRISE DOMAIN CONTROLLERS |
| Description | WS-01\ENTERPRISE DOMAIN CONTROLLERS |
| Domain | WS-01 |
| Local Account | True |
| Name | ENTERPRISE DOMAIN CONTROLLERS |
| SID | S-1-5-9 |
| SID Type | Well Known Group |
| ------ BLOCK 11 ------ | |
| Caption | WS-01\Everyone |
| Description | WS-01\Everyone |
| Domain | WS-01 |
| Local Account | True |
| Name | Everyone |
| SID | S-1-1-0 |
| SID Type | Well Known Group |
| ------ BLOCK 12 ------ | |
| Caption | WS-01\INTERACTIVE |
| Description | WS-01\INTERACTIVE |
| Domain | WS-01 |
| Local Account | True |
| Name | INTERACTIVE |
| SID | S-1-5-4 |
| SID Type | Well Known Group |
| ------ BLOCK 13 ------ | |
| Caption | WS-01\IUSR |
| Description | WS-01\IUSR |
| Domain | WS-01 |
| Local Account | True |
| Name | IUSR |
| SID | S-1-5-17 |
| SID Type | Well Known Group |
| ------ BLOCK 14 ------ | |
| Caption | WS-01\LOCAL |
| Description | WS-01\LOCAL |
| Domain | WS-01 |
| Local Account | True |
| Name | LOCAL |
| SID | S-1-2-0 |
| SID Type | Well Known Group |
| ------ BLOCK 15 ------ | |
| Caption | WS-01\LOCAL SERVICE |
| Description | WS-01\LOCAL SERVICE |
| Domain | WS-01 |
| Local Account | True |
| Name | LOCAL SERVICE |
| SID | S-1-5-19 |
| SID Type | Well Known Group |
| ------ BLOCK 16 ------ | |
| Caption | WS-01\NETWORK |
| Description | WS-01\NETWORK |
| Domain | WS-01 |
| Local Account | True |
| Name | NETWORK |
| SID | S-1-5-2 |
| SID Type | Well Known Group |
| ------ BLOCK 17 ------ | |
| Caption | WS-01\NETWORK SERVICE |
| Description | WS-01\NETWORK SERVICE |
| Domain | WS-01 |
| Local Account | True |
| Name | NETWORK SERVICE |
| SID | S-1-5-20 |
| SID Type | Well Known Group |
| ------ BLOCK 18 ------ | |
| Caption | WS-01\OWNER RIGHTS |
| Description | WS-01\OWNER RIGHTS |
| Domain | WS-01 |
| Local Account | True |
| Name | OWNER RIGHTS |
| SID | S-1-3-4 |
| SID Type | Well Known Group |
| ------ BLOCK 19 ------ | |
| Caption | WS-01\PROXY |
| Description | WS-01\PROXY |
| Domain | WS-01 |
| Local Account | True |
| Name | PROXY |
| SID | S-1-5-8 |
| SID Type | Well Known Group |
| ------ BLOCK 20 ------ | |
| Caption | WS-01\REMOTE INTERACTIVE LOGON |
| Description | WS-01\REMOTE INTERACTIVE LOGON |
| Domain | WS-01 |
| Local Account | True |
| Name | REMOTE INTERACTIVE LOGON |
| SID | S-1-5-14 |
| SID Type | Well Known Group |
| ------ BLOCK 21 ------ | |
| Caption | WS-01\RESTRICTED |
| Description | WS-01\RESTRICTED |
| Domain | WS-01 |
| Local Account | True |
| Name | RESTRICTED |
| SID | S-1-5-12 |
| SID Type | Well Known Group |
| ------ BLOCK 22 ------ | |
| Caption | WS-01\SELF |
| Description | WS-01\SELF |
| Domain | WS-01 |
| Local Account | True |
| Name | SELF |
| SID | S-1-5-10 |
| SID Type | Well Known Group |
| ------ BLOCK 23 ------ | |
| Caption | WS-01\SERVICE |
| Description | WS-01\SERVICE |
| Domain | WS-01 |
| Local Account | True |
| Name | SERVICE |
| SID | S-1-5-6 |
| SID Type | Well Known Group |
| ------ BLOCK 24 ------ | |
| Caption | WS-01\SYSTEM |
| Description | WS-01\SYSTEM |
| Domain | WS-01 |
| Local Account | True |
| Name | SYSTEM |
| SID | S-1-5-18 |
| SID Type | Well Known Group |
| ------ BLOCK 25 ------ | |
| Caption | WS-01\TERMINAL SERVER USER |
| Description | WS-01\TERMINAL SERVER USER |
| Domain | WS-01 |
| Local Account | True |
| Name | TERMINAL SERVER USER |
| SID | S-1-5-13 |
| SID Type | Well Known Group |

Table 30: [WMI] System Account (Detailed)

# [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 31: [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 32: [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 33: [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 34: [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 35: [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 36: [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

## Basic

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

Table 37: [WMI] Printer (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Capability Descriptions | Color Duplex |
| Default | False |
| Device ID | Fax |
| Driver Name | Microsoft Shared Fax Driver |
| Hidden | False |
| Local | True |
| Name | Fax |
| Network | False |
| PNP Device ID |  |
| Port Name | SHRFAX: |
| Print Processor | winprint |
| Server Name |  |
| Share Name |  |
| Shared | False |
| ------ BLOCK 2 ------ | |
| Capability Descriptions | Copies Color |
| Default | False |
| Device ID | Microsoft Print to PDF |
| Driver Name | Microsoft Print To PDF |
| Hidden | False |
| Local | True |
| Name | Microsoft Print to PDF |
| Network | False |
| PNP Device ID |  |
| Port Name | PORTPROMPT: |
| Print Processor | winprint |
| Server Name |  |
| Share Name |  |
| Shared | False |
| ------ BLOCK 3 ------ | |
| Capability Descriptions | Copies Color Collate |
| Default | False |
| Device ID | Microsoft XPS Document Writer |
| Driver Name | Microsoft XPS Document Writer v4 |
| Hidden | False |
| Local | True |
| Name | Microsoft XPS Document Writer |
| Network | False |
| PNP Device ID |  |
| Port Name | PORTPROMPT: |
| Print Processor | winprint |
| Server Name |  |
| Share Name |  |
| Shared | False |

Table 38: [WMI] Printer (Detailed)

# [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 39: [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 40: [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 41: [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 42: [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 43: [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 44: [WMI] Optional Features

# [WMI] Services

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

| Name | Start Mode | Start Name | State |
| --- | --- | --- | --- |
| AarSvc\_49269 | Manual |  | Stopped |
| AJRouter | Manual | NT AUTHORITY\LocalService | Stopped |
| ALG | Manual | NT AUTHORITY\LocalService | Stopped |
| AppIDSvc | Manual | NT Authority\LocalService | Stopped |
| Appinfo | Manual | LocalSystem | Running |
| AppMgmt | Manual | LocalSystem | Stopped |
| AppReadiness | Manual | LocalSystem | Stopped |
| AppVClient | Disabled | LocalSystem | Stopped |
| AppXSvc | Manual | LocalSystem | Stopped |
| AssignedAccessManagerSvc | Manual | LocalSystem | Stopped |
| AudioEndpointBuilder | Auto | LocalSystem | Running |
| Audiosrv | Auto | NT AUTHORITY\LocalService | Running |
| autotimesvc | Manual | NT AUTHORITY\LocalService | Stopped |
| AxInstSV | Manual | LocalSystem | Stopped |
| BcastDVRUserService\_49269 | Manual |  | Stopped |
| BDESVC | Manual | localSystem | Stopped |
| BFE | Auto | NT AUTHORITY\LocalService | Running |
| BITS | Manual | LocalSystem | Stopped |
| BluetoothUserService\_49269 | Manual |  | Stopped |
| BrokerInfrastructure | Auto | LocalSystem | Running |
| BTAGService | Manual | NT AUTHORITY\LocalService | Stopped |
| BthAvctpSvc | Manual | NT AUTHORITY\LocalService | Running |
| bthserv | Manual | NT AUTHORITY\LocalService | Stopped |
| camsvc | Manual | LocalSystem | Stopped |
| CaptureService\_49269 | Manual |  | Stopped |
| cbdhsvc\_49269 | Manual |  | Running |
| CDPSvc | Auto | NT AUTHORITY\LocalService | Running |
| CDPUserSvc\_49269 | Auto |  | Running |
| CertPropSvc | Manual | LocalSystem | Running |
| ClipSVC | Manual | LocalSystem | Stopped |
| COMSysApp | Manual | LocalSystem | Stopped |
| ConsentUxUserSvc\_49269 | Manual |  | Stopped |
| CoreMessagingRegistrar | Auto | NT AUTHORITY\LocalService | Running |
| CredentialEnrollmentManagerUserSvc\_49269 | Manual |  | Stopped |
| CryptSvc | Auto | NT Authority\NetworkService | Running |
| CscService | Manual | LocalSystem | Stopped |
| DcomLaunch | Auto | LocalSystem | Running |
| defragsvc | Manual | localSystem | Stopped |
| DeviceAssociationBrokerSvc\_49269 | Manual |  | Stopped |
| DeviceAssociationService | Manual | LocalSystem | Stopped |
| DeviceInstall | Manual | LocalSystem | Stopped |
| DevicePickerUserSvc\_49269 | Manual |  | Stopped |
| DevicesFlowUserSvc\_49269 | Manual |  | Stopped |
| DevQueryBroker | Manual | LocalSystem | Stopped |
| Dhcp | Auto | NT Authority\LocalService | Running |
| diagnosticshub.standardcollector.service | Manual | LocalSystem | Stopped |
| diagsvc | Manual | LocalSystem | Stopped |
| DiagTrack | Auto | LocalSystem | Running |
| DispBrokerDesktopSvc | Auto | NT AUTHORITY\LocalService | Running |
| DisplayEnhancementService | Manual | LocalSystem | Stopped |
| DmEnrollmentSvc | Manual | LocalSystem | Stopped |
| dmwappushservice | Manual | LocalSystem | Stopped |
| Dnscache | Auto | NT AUTHORITY\NetworkService | Running |
| DoSvc | Auto | NT Authority\NetworkService | Stopped |
| dot3svc | Manual | localSystem | Stopped |
| DPS | Auto | NT AUTHORITY\LocalService | Running |
| DsmSvc | Manual | LocalSystem | Running |
| DsSvc | Manual | LocalSystem | Stopped |
| DusmSvc | Auto | NT Authority\LocalService | Running |
| Eaphost | Manual | localSystem | Stopped |
| edgeupdate | Auto | LocalSystem | Stopped |
| edgeupdatem | Manual | LocalSystem | Stopped |
| EFS | Manual | LocalSystem | Stopped |
| embeddedmode | Manual | LocalSystem | Stopped |
| EntAppSvc | Manual | LocalSystem | Stopped |
| EventLog | Auto | NT AUTHORITY\LocalService | Running |
| EventSystem | Auto | NT AUTHORITY\LocalService | Running |
| Fax | Manual | NT AUTHORITY\NetworkService | Stopped |
| fdPHost | Manual | NT AUTHORITY\LocalService | Stopped |
| FDResPub | Manual | NT AUTHORITY\LocalService | Stopped |
| fhsvc | Manual | LocalSystem | Stopped |
| FontCache | Auto | NT AUTHORITY\LocalService | Running |
| FrameServer | Manual | LocalSystem | Stopped |
| gpsvc | Auto | LocalSystem | Stopped |
| GraphicsPerfSvc | Manual | LocalSystem | Stopped |
| hidserv | Manual | LocalSystem | Stopped |
| HvHost | Manual | LocalSystem | Stopped |
| icssvc | Manual | NT Authority\LocalService | Stopped |
| IKEEXT | Auto | LocalSystem | Running |
| InstallService | Manual | LocalSystem | Running |
| iphlpsvc | Auto | LocalSystem | Running |
| IpxlatCfgSvc | Manual | LocalSystem | Stopped |
| KeyIso | Manual | LocalSystem | Running |
| KtmRm | Manual | NT AUTHORITY\NetworkService | Stopped |
| LanmanServer | Auto | LocalSystem | Running |
| LanmanWorkstation | Auto | NT AUTHORITY\NetworkService | Running |
| lfsvc | Manual | LocalSystem | Stopped |
| LicenseManager | Manual | NT Authority\LocalService | Running |
| lltdsvc | Manual | NT AUTHORITY\LocalService | Stopped |
| lmhosts | Manual | NT AUTHORITY\LocalService | Running |
| LSM | Auto | LocalSystem | Running |
| LxpSvc | Manual | LocalSystem | Stopped |
| MapsBroker | Auto | NT AUTHORITY\NetworkService | Stopped |
| MessagingService\_49269 | Manual |  | Stopped |
| MicrosoftEdgeElevationService | Manual | LocalSystem | Stopped |
| MixedRealityOpenXRSvc | Manual | LocalSystem | Stopped |
| mpssvc | Auto | NT Authority\LocalService | Running |
| MSDTC | Manual | NT AUTHORITY\NetworkService | Stopped |
| MSiSCSI | Manual | LocalSystem | Stopped |
| msiserver | Manual | LocalSystem | Stopped |
| NaturalAuthentication | Manual | LocalSystem | Stopped |
| NcaSvc | Manual | LocalSystem | Stopped |
| NcbService | Manual | LocalSystem | Running |
| NcdAutoSetup | Manual | NT AUTHORITY\LocalService | Stopped |
| Netlogon | Auto | LocalSystem | Running |
| Netman | Manual | LocalSystem | Stopped |
| netprofm | Manual | NT AUTHORITY\LocalService | Running |
| NetSetupSvc | Manual | LocalSystem | Stopped |
| NetTcpPortSharing | Disabled | NT AUTHORITY\LocalService | Stopped |
| NgcCtnrSvc | Manual | NT AUTHORITY\LocalService | Stopped |
| NgcSvc | Manual | LocalSystem | Stopped |
| NlaSvc | Auto | NT AUTHORITY\NetworkService | Running |
| nsi | Auto | NT Authority\LocalService | Running |
| OneSyncSvc\_49269 | Auto |  | Running |
| p2pimsvc | Manual | NT AUTHORITY\LocalService | Stopped |
| p2psvc | Manual | NT AUTHORITY\LocalService | Stopped |
| PcaSvc | Manual | LocalSystem | Running |
| PeerDistSvc | Manual | NT AUTHORITY\NetworkService | Stopped |
| perceptionsimulation | Manual | LocalSystem | Stopped |
| PerfHost | Manual | NT AUTHORITY\LocalService | Stopped |
| PhoneSvc | Manual | NT Authority\LocalService | Stopped |
| PimIndexMaintenanceSvc\_49269 | Manual |  | Stopped |
| pla | Manual | NT AUTHORITY\LocalService | Stopped |
| PlugPlay | Manual | LocalSystem | Running |
| PNRPAutoReg | Manual | NT AUTHORITY\LocalService | Stopped |
| PNRPsvc | Manual | NT AUTHORITY\LocalService | Stopped |
| PolicyAgent | Manual | NT Authority\NetworkService | Running |
| Power | Auto | LocalSystem | Running |
| PrintNotify | Manual | LocalSystem | Stopped |
| PrintWorkflowUserSvc\_49269 | Manual |  | Stopped |
| ProfSvc | Auto | LocalSystem | Running |
| PushToInstall | Manual | LocalSystem | Stopped |
| QWAVE | Manual | NT AUTHORITY\LocalService | Stopped |
| RasAuto | Manual | localSystem | Stopped |
| RasMan | Manual | localSystem | Stopped |
| RemoteAccess | Disabled | localSystem | Stopped |
| RemoteRegistry | Auto | NT AUTHORITY\LocalService | Running |
| RetailDemo | Manual | LocalSystem | Stopped |
| RmSvc | Manual | NT AUTHORITY\LocalService | Running |
| RpcEptMapper | Auto | NT AUTHORITY\NetworkService | Running |
| RpcLocator | Manual | NT AUTHORITY\NetworkService | Stopped |
| RpcSs | Auto | NT AUTHORITY\NetworkService | Running |
| SamSs | Auto | LocalSystem | Running |
| SCardSvr | Manual | NT AUTHORITY\LocalService | Stopped |
| ScDeviceEnum | Manual | LocalSystem | Running |
| Schedule | Auto | LocalSystem | Running |
| SCPolicySvc | Manual | LocalSystem | Stopped |
| SDRSVC | Manual | localSystem | Stopped |
| seclogon | Manual | LocalSystem | Stopped |
| SecurityHealthService | Manual | LocalSystem | Running |
| SEMgrSvc | Manual | NT AUTHORITY\LocalService | Running |
| SENS | Auto | LocalSystem | Running |
| Sense | Manual | LocalSystem | Stopped |
| SensorDataService | Manual | LocalSystem | Stopped |
| SensorService | Manual | LocalSystem | Stopped |
| SensrSvc | Manual | NT AUTHORITY\LocalService | Stopped |
| SessionEnv | Manual | localSystem | Running |
| SgrmBroker | Auto | LocalSystem | Running |
| SharedAccess | Manual | LocalSystem | Stopped |
| SharedRealitySvc | Manual | NT AUTHORITY\LocalService | Stopped |
| ShellHWDetection | Auto | LocalSystem | Running |
| shpamsvc | Disabled | LocalSystem | Stopped |
| smphost | Manual | NT AUTHORITY\NetworkService | Stopped |
| SmsRouter | Manual | NT Authority\LocalService | Running |
| SNMPTRAP | Manual | NT AUTHORITY\LocalService | Stopped |
| spectrum | Manual | NT AUTHORITY\LocalService | Stopped |
| Spooler | Auto | LocalSystem | Running |
| sppsvc | Auto | NT AUTHORITY\NetworkService | Stopped |
| SSDPSRV | Manual | NT AUTHORITY\LocalService | Stopped |
| ssh-agent | Disabled | LocalSystem | Stopped |
| SstpSvc | Manual | NT Authority\LocalService | Stopped |
| StateRepository | Manual | LocalSystem | Running |
| stisvc | Manual | NT Authority\LocalService | Stopped |
| StorSvc | Auto | LocalSystem | Running |
| svsvc | Manual | LocalSystem | Stopped |
| swprv | Manual | LocalSystem | Stopped |
| SysMain | Auto | LocalSystem | Running |
| SystemEventsBroker | Auto | LocalSystem | Running |
| TabletInputService | Manual | LocalSystem | Running |
| TapiSrv | Manual | NT AUTHORITY\NetworkService | Stopped |
| TermService | Manual | NT Authority\NetworkService | Running |
| Themes | Auto | LocalSystem | Running |
| TieringEngineService | Manual | localSystem | Stopped |
| TimeBrokerSvc | Manual | NT AUTHORITY\LocalService | Running |
| TokenBroker | Manual | LocalSystem | Running |
| TrkWks | Auto | LocalSystem | Running |
| TroubleshootingSvc | Manual | LocalSystem | Stopped |
| TrustedInstaller | Manual | localSystem | Running |
| tzautoupdate | Disabled | NT AUTHORITY\LocalService | Stopped |
| UdkUserSvc\_49269 | Manual |  | Stopped |
| UevAgentService | Disabled | LocalSystem | Stopped |
| UmRdpService | Manual | localSystem | Running |
| UnistoreSvc\_49269 | Manual |  | Stopped |
| upnphost | Manual | NT AUTHORITY\LocalService | Stopped |
| UserDataSvc\_49269 | Manual |  | Stopped |
| UserManager | Auto | LocalSystem | Running |
| UsoSvc | Auto | LocalSystem | Running |
| VacSvc | Manual | NT AUTHORITY\LocalService | Stopped |
| VaultSvc | Manual | LocalSystem | Running |
| vds | Manual | LocalSystem | Stopped |
| vmicguestinterface | Manual | LocalSystem | Running |
| vmicheartbeat | Manual | LocalSystem | Running |
| vmickvpexchange | Manual | LocalSystem | Running |
| vmicrdv | Manual | LocalSystem | Running |
| vmicshutdown | Manual | LocalSystem | Running |
| vmictimesync | Manual | NT AUTHORITY\LocalService | Running |
| vmicvmsession | Manual | LocalSystem | Stopped |
| vmicvss | Manual | LocalSystem | Running |
| VSS | Manual | LocalSystem | Running |
| W32Time | Manual | NT AUTHORITY\LocalService | Running |
| WaaSMedicSvc | Manual | LocalSystem | Running |
| WalletService | Manual | LocalSystem | Stopped |
| WarpJITSvc | Manual | NT Authority\LocalService | Stopped |
| wbengine | Manual | localSystem | Stopped |
| WbioSrvc | Manual | LocalSystem | Stopped |
| Wcmsvc | Auto | NT Authority\LocalService | Running |
| wcncsvc | Manual | NT AUTHORITY\LocalService | Stopped |
| WdiServiceHost | Manual | NT AUTHORITY\LocalService | Running |
| WdiSystemHost | Manual | LocalSystem | Stopped |
| WdNisSvc | Manual | NT AUTHORITY\LocalService | Running |
| WebClient | Manual | NT AUTHORITY\LocalService | Stopped |
| Wecsvc | Manual | NT AUTHORITY\NetworkService | Stopped |
| WEPHOSTSVC | Manual | NT AUTHORITY\LocalService | Stopped |
| wercplsupport | Manual | localSystem | Stopped |
| WerSvc | Manual | localSystem | Stopped |
| WFDSConMgrSvc | Manual | NT AUTHORITY\LocalService | Stopped |
| WiaRpc | Manual | LocalSystem | Stopped |
| WinDefend | Auto | LocalSystem | Running |
| WinHttpAutoProxySvc | Manual | NT AUTHORITY\LocalService | Running |
| Winmgmt | Auto | localSystem | Running |
| WinRM | Auto | NT AUTHORITY\NetworkService | Running |
| wisvc | Manual | LocalSystem | Stopped |
| WlanSvc | Manual | LocalSystem | Stopped |
| wlidsvc | Manual | LocalSystem | Stopped |
| wlpasvc | Manual | NT Authority\LocalService | Stopped |
| WManSvc | Manual | LocalSystem | Stopped |
| wmiApSrv | Manual | localSystem | Stopped |
| WMPNetworkSvc | Manual | NT AUTHORITY\NetworkService | Stopped |
| workfolderssvc | Manual | NT AUTHORITY\LocalService | Stopped |
| WpcMonSvc | Manual | LocalSystem | Stopped |
| WPDBusEnum | Manual | LocalSystem | Stopped |
| WpnService | Auto | LocalSystem | Running |
| WpnUserService\_49269 | Auto |  | Running |
| wscsvc | Auto | NT AUTHORITY\LocalService | Running |
| WSearch | Auto | LocalSystem | Running |
| wuauserv | Manual | LocalSystem | Running |
| WwanSvc | Manual | localSystem | Stopped |
| XblAuthManager | Manual | LocalSystem | Stopped |
| XblGameSave | Manual | LocalSystem | Stopped |
| XboxGipSvc | Manual | LocalSystem | Stopped |
| XboxNetApiSvc | Manual | LocalSystem | Stopped |

Table 45: [WMI] Services

# [WMI] Processes

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

| Name | Description |
| --- | --- |
| ApplicationFrameHost.exe | ApplicationFrameHost.exe |
| csrss.exe | csrss.exe |
| csrss.exe | csrss.exe |
| csrss.exe | csrss.exe |
| ctfmon.exe | ctfmon.exe |
| dllhost.exe | dllhost.exe |
| dllhost.exe | dllhost.exe |
| dllhost.exe | dllhost.exe |
| dwm.exe | dwm.exe |
| dwm.exe | dwm.exe |
| explorer.exe | explorer.exe |
| explorer.exe | explorer.exe |
| fontdrvhost.exe | fontdrvhost.exe |
| fontdrvhost.exe | fontdrvhost.exe |
| fontdrvhost.exe | fontdrvhost.exe |
| LogonUI.exe | LogonUI.exe |
| lsass.exe | lsass.exe |
| Memory Compression | Memory Compression |
| Microsoft.Photos.exe | Microsoft.Photos.exe |
| MoUsoCoreWorker.exe | MoUsoCoreWorker.exe |
| MsMpEng.exe | MsMpEng.exe |
| NisSrv.exe | NisSrv.exe |
| notepad.exe | notepad.exe |
| OneDrive.exe | OneDrive.exe |
| rdpclip.exe | rdpclip.exe |
| rdpinput.exe | rdpinput.exe |
| Registry | Registry |
| RuntimeBroker.exe | RuntimeBroker.exe |
| RuntimeBroker.exe | RuntimeBroker.exe |
| RuntimeBroker.exe | RuntimeBroker.exe |
| RuntimeBroker.exe | RuntimeBroker.exe |
| RuntimeBroker.exe | RuntimeBroker.exe |
| RuntimeBroker.exe | RuntimeBroker.exe |
| SearchApp.exe | SearchApp.exe |
| SearchIndexer.exe | SearchIndexer.exe |
| SecurityHealthService.exe | SecurityHealthService.exe |
| SecurityHealthSystray.exe | SecurityHealthSystray.exe |
| services.exe | services.exe |
| SgrmBroker.exe | SgrmBroker.exe |
| ShellExperienceHost.exe | ShellExperienceHost.exe |
| sihost.exe | sihost.exe |
| SkypeApp.exe | SkypeApp.exe |
| SkypeBackgroundHost.exe | SkypeBackgroundHost.exe |
| smss.exe | smss.exe |
| spoolsv.exe | spoolsv.exe |
| StartMenuExperienceHost.exe | StartMenuExperienceHost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| svchost.exe | svchost.exe |
| System | System |
| System Idle Process | System Idle Process |
| TabTip.exe | TabTip.exe |
| taskhostw.exe | taskhostw.exe |
| TextInputHost.exe | TextInputHost.exe |
| TiWorker.exe | TiWorker.exe |
| TrustedInstaller.exe | TrustedInstaller.exe |
| VSSVC.exe | VSSVC.exe |
| wininit.exe | wininit.exe |
| winlogon.exe | winlogon.exe |
| winlogon.exe | winlogon.exe |
| WmiPrvSE.exe | WmiPrvSE.exe |
| WUDFHost.exe | WUDFHost.exe |

Table 46: [WMI] Processes

# [WMI] System Drivers

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

| Name | Service Type | Start Mode | Started | State |
| --- | --- | --- | --- | --- |
| 1394ohci | Kernel Driver | Manual | False | Stopped |
| 3ware | Kernel Driver | Manual | False | Stopped |
| ACPI | Kernel Driver | Boot | True | Running |
| AcpiDev | Kernel Driver | Manual | False | Stopped |
| acpiex | Kernel Driver | Boot | True | Running |
| acpipagr | Kernel Driver | Manual | False | Stopped |
| AcpiPmi | Kernel Driver | Manual | False | Stopped |
| acpitime | Kernel Driver | Manual | False | Stopped |
| Acx01000 | Kernel Driver | Manual | False | Stopped |
| ADP80XX | Kernel Driver | Manual | False | Stopped |
| AFD | Kernel Driver | System | True | Running |
| afunix | Kernel Driver | System | True | Running |
| ahcache | Kernel Driver | System | True | Running |
| amdgpio2 | Kernel Driver | Manual | False | Stopped |
| amdi2c | Kernel Driver | Manual | False | Stopped |
| AmdK8 | Kernel Driver | Manual | False | Stopped |
| AmdPPM | Kernel Driver | Manual | True | Running |
| amdsata | Kernel Driver | Manual | False | Stopped |
| amdsbs | Kernel Driver | Manual | False | Stopped |
| amdxata | Kernel Driver | Manual | False | Stopped |
| AppID | Kernel Driver | Manual | False | Stopped |
| applockerfltr | Kernel Driver | Manual | False | Stopped |
| AppvStrm | File System Driver | Manual | False | Stopped |
| AppvVemgr | File System Driver | Manual | False | Stopped |
| AppvVfs | File System Driver | Manual | False | Stopped |
| arcsas | Kernel Driver | Manual | False | Stopped |
| AsyncMac | Kernel Driver | Manual | False | Stopped |
| atapi | Kernel Driver | Manual | False | Stopped |
| b06bdrv | Kernel Driver | Manual | False | Stopped |
| bam | Kernel Driver | System | True | Running |
| BasicDisplay | Kernel Driver | System | True | Running |
| BasicRender | Kernel Driver | System | True | Running |
| bcmfn2 | Kernel Driver | Manual | False | Stopped |
| Beep | Kernel Driver | System | True | Running |
| bindflt | File System Driver | Auto | True | Running |
| bowser | File System Driver | Manual | True | Running |
| BthA2dp | Kernel Driver | Manual | False | Stopped |
| BthEnum | Kernel Driver | Manual | False | Stopped |
| BthHFEnum | Kernel Driver | Manual | False | Stopped |
| BthLEEnum | Kernel Driver | Manual | False | Stopped |
| BthMini | Kernel Driver | Manual | False | Stopped |
| BTHMODEM | Kernel Driver | Manual | False | Stopped |
| BTHPORT | Kernel Driver | Manual | False | Stopped |
| BTHUSB | Kernel Driver | Manual | False | Stopped |
| bttflt | Kernel Driver | Manual | False | Stopped |
| buttonconverter | Kernel Driver | Manual | False | Stopped |
| CAD | Kernel Driver | Manual | True | Running |
| cdfs | File System Driver | Disabled | False | Stopped |
| cdrom | Kernel Driver | System | True | Running |
| cht4iscsi | Kernel Driver | Manual | False | Stopped |
| cht4vbd | Kernel Driver | Manual | False | Stopped |
| CimFS | File System Driver | System | True | Running |
| circlass | Kernel Driver | Manual | False | Stopped |
| CldFlt | File System Driver | Auto | True | Running |
| CLFS | Kernel Driver | Boot | True | Running |
| CmBatt | Kernel Driver | Manual | True | Running |
| CNG | Kernel Driver | Boot | True | Running |
| cnghwassist | Kernel Driver | Disabled | False | Stopped |
| CompositeBus | Kernel Driver | Manual | True | Running |
| condrv | Kernel Driver | Manual | True | Running |
| CSC | Kernel Driver | System | True | Running |
| dam | Kernel Driver | System | False | Stopped |
| Dfsc | File System Driver | System | True | Running |
| disk | Kernel Driver | Boot | True | Running |
| dmvsc | Kernel Driver | Manual | True | Running |
| drmkaud | Kernel Driver | Manual | False | Stopped |
| DXGKrnl | Kernel Driver | System | True | Running |
| ebdrv | Kernel Driver | Manual | False | Stopped |
| EhStorClass | Kernel Driver | Boot | True | Running |
| EhStorTcgDrv | Kernel Driver | Manual | False | Stopped |
| ErrDev | Kernel Driver | Manual | False | Stopped |
| exfat | File System Driver | Manual | False | Stopped |
| fastfat | File System Driver | Manual | True | Running |
| fdc | Kernel Driver | Manual | False | Stopped |
| FileCrypt | File System Driver | System | True | Running |
| FileInfo | File System Driver | Boot | True | Running |
| Filetrace | File System Driver | Manual | False | Stopped |
| flpydisk | Kernel Driver | Manual | False | Stopped |
| FltMgr | File System Driver | Boot | True | Running |
| FsDepends | File System Driver | Manual | False | Stopped |
| fvevol | Kernel Driver | Boot | True | Running |
| gencounter | Kernel Driver | Manual | True | Running |
| genericusbfn | Kernel Driver | Manual | False | Stopped |
| GPIOClx0101 | Kernel Driver | Manual | False | Stopped |
| GpuEnergyDrv | Kernel Driver | System | True | Running |
| HdAudAddService | Kernel Driver | Manual | False | Stopped |
| HDAudBus | Kernel Driver | Manual | False | Stopped |
| HidBatt | Kernel Driver | Manual | False | Stopped |
| HidBth | Kernel Driver | Manual | False | Stopped |
| hidi2c | Kernel Driver | Manual | False | Stopped |
| hidinterrupt | Kernel Driver | Manual | False | Stopped |
| HidIr | Kernel Driver | Manual | False | Stopped |
| hidspi | Kernel Driver | Manual | False | Stopped |
| HidUsb | Kernel Driver | Manual | False | Stopped |
| HpSAMD | Kernel Driver | Manual | False | Stopped |
| HTTP | Kernel Driver | Manual | True | Running |
| hvcrash | Kernel Driver | Disabled | False | Stopped |
| hvservice | Kernel Driver | Manual | False | Stopped |
| HwNClx0101 | Kernel Driver | Manual | False | Stopped |
| hwpolicy | Kernel Driver | Boot | False | Stopped |
| hyperkbd | Kernel Driver | Manual | True | Running |
| HyperVideo | Kernel Driver | Manual | True | Running |
| i8042prt | Kernel Driver | Manual | False | Stopped |
| iagpio | Kernel Driver | Manual | False | Stopped |
| iai2c | Kernel Driver | Manual | False | Stopped |
| iaLPSS2i\_GPIO2 | Kernel Driver | Manual | False | Stopped |
| iaLPSS2i\_GPIO2\_BXT\_P | Kernel Driver | Manual | False | Stopped |
| iaLPSS2i\_GPIO2\_CNL | Kernel Driver | Manual | False | Stopped |
| iaLPSS2i\_GPIO2\_GLK | Kernel Driver | Manual | False | Stopped |
| iaLPSS2i\_I2C | Kernel Driver | Manual | False | Stopped |
| iaLPSS2i\_I2C\_BXT\_P | Kernel Driver | Manual | False | Stopped |
| iaLPSS2i\_I2C\_CNL | Kernel Driver | Manual | False | Stopped |
| iaLPSS2i\_I2C\_GLK | Kernel Driver | Manual | False | Stopped |
| iaLPSSi\_GPIO | Kernel Driver | Manual | False | Stopped |
| iaLPSSi\_I2C | Kernel Driver | Manual | False | Stopped |
| iaStorAVC | Kernel Driver | Manual | False | Stopped |
| iaStorV | Kernel Driver | Manual | False | Stopped |
| ibbus | Kernel Driver | Manual | False | Stopped |
| IndirectKmd | Kernel Driver | Manual | True | Running |
| intelide | Kernel Driver | Manual | False | Stopped |
| intelpep | Kernel Driver | Boot | True | Running |
| intelpmax | Kernel Driver | Manual | False | Stopped |
| intelppm | Kernel Driver | Manual | False | Stopped |
| iorate | Kernel Driver | Boot | True | Running |
| IpFilterDriver | Kernel Driver | Manual | False | Stopped |
| IPMIDRV | Kernel Driver | Manual | False | Stopped |
| IPNAT | Kernel Driver | Manual | False | Stopped |
| IPT | Kernel Driver | Manual | False | Stopped |
| isapnp | Kernel Driver | Manual | False | Stopped |
| iScsiPrt | Kernel Driver | Manual | False | Stopped |
| ItSas35i | Kernel Driver | Manual | False | Stopped |
| kbdclass | Kernel Driver | Manual | True | Running |
| kbdhid | Kernel Driver | Manual | False | Stopped |
| kdnic | Kernel Driver | Manual | True | Running |
| KSecDD | Kernel Driver | Boot | True | Running |
| KSecPkg | Kernel Driver | Boot | True | Running |
| ksthunk | Kernel Driver | Manual | False | Stopped |
| lltdio | Kernel Driver | Auto | True | Running |
| LSI\_SAS | Kernel Driver | Manual | False | Stopped |
| LSI\_SAS2i | Kernel Driver | Manual | False | Stopped |
| LSI\_SAS3i | Kernel Driver | Manual | False | Stopped |
| LSI\_SSS | Kernel Driver | Manual | False | Stopped |
| luafv | File System Driver | Auto | True | Running |
| mausbhost | Kernel Driver | Manual | False | Stopped |
| mausbip | Kernel Driver | Manual | False | Stopped |
| MbbCx | Kernel Driver | Manual | False | Stopped |
| megasas | Kernel Driver | Manual | False | Stopped |
| megasas2i | Kernel Driver | Manual | False | Stopped |
| megasas35i | Kernel Driver | Manual | False | Stopped |
| megasr | Kernel Driver | Manual | False | Stopped |
| Microsoft\_Bluetooth\_AvrcpTransport | Kernel Driver | Manual | False | Stopped |
| mlx4\_bus | Kernel Driver | Manual | False | Stopped |
| MMCSS | Kernel Driver | Auto | True | Running |
| Modem | Kernel Driver | Manual | False | Stopped |
| monitor | Kernel Driver | Manual | True | Running |
| mouclass | Kernel Driver | Manual | True | Running |
| mouhid | Kernel Driver | Manual | True | Running |
| mountmgr | Kernel Driver | Boot | True | Running |
| mpsdrv | Kernel Driver | Manual | True | Running |
| MRxDAV | File System Driver | Manual | False | Stopped |
| mrxsmb | File System Driver | Manual | True | Running |
| mrxsmb20 | File System Driver | Manual | True | Running |
| MsBridge | Kernel Driver | Manual | False | Stopped |
| Msfs | File System Driver | System | True | Running |
| msgpiowin32 | Kernel Driver | Manual | False | Stopped |
| mshidkmdf | Kernel Driver | Manual | False | Stopped |
| mshidumdf | Kernel Driver | Manual | False | Stopped |
| msisadrv | Kernel Driver | Manual | False | Stopped |
| MSKSSRV | Kernel Driver | Manual | False | Stopped |
| MsLldp | Kernel Driver | Auto | True | Running |
| MSPCLOCK | Kernel Driver | Manual | False | Stopped |
| MSPQM | Kernel Driver | Manual | False | Stopped |
| MsQuic | Kernel Driver | Manual | True | Running |
| MsRPC | Kernel Driver | Manual | False | Stopped |
| MsSecFlt | Kernel Driver | Boot | True | Running |
| mssmbios | Kernel Driver | System | True | Running |
| MSTEE | Kernel Driver | Manual | False | Stopped |
| MTConfig | Kernel Driver | Manual | False | Stopped |
| Mup | File System Driver | Boot | True | Running |
| mvumis | Kernel Driver | Manual | False | Stopped |
| NativeWifiP | Kernel Driver | Manual | False | Stopped |
| ndfltr | Kernel Driver | Manual | False | Stopped |
| NDIS | Kernel Driver | Boot | True | Running |
| NdisCap | Kernel Driver | System | True | Running |
| NdisImPlatform | Kernel Driver | Manual | False | Stopped |
| NdisTapi | Kernel Driver | Manual | False | Stopped |
| Ndisuio | Kernel Driver | Manual | False | Stopped |
| NdisVirtualBus | Kernel Driver | Manual | True | Running |
| NdisWan | Kernel Driver | Manual | False | Stopped |
| ndiswanlegacy | Kernel Driver | Manual | False | Stopped |
| NDKPing | Kernel Driver | Manual | False | Stopped |
| ndproxy | Kernel Driver | Manual | False | Stopped |
| Ndu | Kernel Driver | Auto | True | Running |
| NetAdapterCx | Kernel Driver | Manual | False | Stopped |
| NetBIOS | File System Driver | System | True | Running |
| NetBT | Kernel Driver | System | True | Running |
| netvsc | Kernel Driver | Manual | True | Running |
| Npfs | File System Driver | System | True | Running |
| npsvctrig | Kernel Driver | System | True | Running |
| nsiproxy | Kernel Driver | System | True | Running |
| Ntfs | File System Driver | Manual | True | Running |
| Null | Kernel Driver | System | True | Running |
| nvdimm | Kernel Driver | Manual | False | Stopped |
| nvraid | Kernel Driver | Manual | False | Stopped |
| nvstor | Kernel Driver | Manual | False | Stopped |
| Parport | Kernel Driver | Manual | False | Stopped |
| partmgr | Kernel Driver | Boot | True | Running |
| pci | Kernel Driver | Manual | False | Stopped |
| pciide | Kernel Driver | Manual | False | Stopped |
| pcmcia | Kernel Driver | Manual | False | Stopped |
| pcw | Kernel Driver | Boot | True | Running |
| pdc | Kernel Driver | Boot | True | Running |
| PEAUTH | Kernel Driver | Auto | True | Running |
| percsas2i | Kernel Driver | Manual | False | Stopped |
| percsas3i | Kernel Driver | Manual | False | Stopped |
| PktMon | Kernel Driver | Manual | False | Stopped |
| pmem | Kernel Driver | Manual | False | Stopped |
| PNPMEM | Kernel Driver | Manual | False | Stopped |
| portcfg | Kernel Driver | Manual | False | Stopped |
| PptpMiniport | Kernel Driver | Manual | False | Stopped |
| Processor | Kernel Driver | Manual | False | Stopped |
| Psched | Kernel Driver | System | True | Running |
| QWAVEdrv | Kernel Driver | Manual | False | Stopped |
| Ramdisk | Kernel Driver | Manual | False | Stopped |
| RasAcd | Kernel Driver | Manual | False | Stopped |
| RasAgileVpn | Kernel Driver | Manual | False | Stopped |
| Rasl2tp | Kernel Driver | Manual | False | Stopped |
| RasPppoe | Kernel Driver | Manual | False | Stopped |
| RasSstp | Kernel Driver | Manual | False | Stopped |
| rdbss | File System Driver | System | True | Running |
| rdpbus | Kernel Driver | Manual | True | Running |
| RDPDR | Kernel Driver | Manual | True | Running |
| RdpVideoMiniport | Kernel Driver | Manual | True | Running |
| rdyboost | Kernel Driver | Boot | True | Running |
| ReFS | File System Driver | Manual | False | Stopped |
| ReFSv1 | File System Driver | Manual | False | Stopped |
| RFCOMM | Kernel Driver | Manual | False | Stopped |
| rhproxy | Kernel Driver | Manual | False | Stopped |
| rspndr | Kernel Driver | Auto | True | Running |
| s3cap | Kernel Driver | Manual | False | Stopped |
| sbp2port | Kernel Driver | Manual | False | Stopped |
| scfilter | Kernel Driver | Manual | False | Stopped |
| scmbus | Kernel Driver | Manual | False | Stopped |
| sdbus | Kernel Driver | Manual | True | Running |
| SDFRd | Kernel Driver | Manual | False | Stopped |
| sdstor | Kernel Driver | Manual | True | Running |
| SerCx | Kernel Driver | Manual | False | Stopped |
| SerCx2 | Kernel Driver | Manual | False | Stopped |
| Serenum | Kernel Driver | Manual | False | Stopped |
| Serial | Kernel Driver | Manual | False | Stopped |
| sermouse | Kernel Driver | Manual | False | Stopped |
| sfloppy | Kernel Driver | Manual | False | Stopped |
| SgrmAgent | Kernel Driver | Boot | True | Running |
| SiSRaid2 | Kernel Driver | Manual | False | Stopped |
| SiSRaid4 | Kernel Driver | Manual | False | Stopped |
| SmartSAMD | Kernel Driver | Manual | False | Stopped |
| smbdirect | File System Driver | Manual | False | Stopped |
| spaceparser | Kernel Driver | Manual | False | Stopped |
| spaceport | Kernel Driver | Boot | True | Running |
| SpatialGraphFilter | Kernel Driver | Manual | False | Stopped |
| SpbCx | Kernel Driver | Manual | False | Stopped |
| srv2 | File System Driver | Manual | True | Running |
| srvnet | File System Driver | Manual | True | Running |
| stexstor | Kernel Driver | Manual | False | Stopped |
| storahci | Kernel Driver | Manual | False | Stopped |
| storflt | Kernel Driver | Manual | False | Stopped |
| stornvme | Kernel Driver | Manual | False | Stopped |
| storqosflt | File System Driver | Auto | True | Running |
| storufs | Kernel Driver | Manual | False | Stopped |
| storvsc | Kernel Driver | Boot | True | Running |
| swenum | Kernel Driver | Manual | True | Running |
| Synth3dVsc | Kernel Driver | Manual | False | Stopped |
| Tcpip | Kernel Driver | Boot | True | Running |
| Tcpip6 | Kernel Driver | Manual | False | Stopped |
| tcpipreg | Kernel Driver | Auto | True | Running |
| tdx | Kernel Driver | System | True | Running |
| Telemetry | Kernel Driver | Boot | True | Running |
| terminpt | Kernel Driver | Manual | True | Running |
| TPM | Kernel Driver | Manual | False | Stopped |
| TsUsbFlt | Kernel Driver | Manual | False | Stopped |
| TsUsbGD | Kernel Driver | Manual | False | Stopped |
| tsusbhub | Kernel Driver | Manual | True | Running |
| tunnel | Kernel Driver | Manual | False | Stopped |
| UASPStor | Kernel Driver | Manual | True | Running |
| UcmCx0101 | Kernel Driver | Manual | False | Stopped |
| UcmTcpciCx0101 | Kernel Driver | Manual | False | Stopped |
| UcmUcsiAcpiClient | Kernel Driver | Manual | False | Stopped |
| UcmUcsiCx0101 | Kernel Driver | Manual | False | Stopped |
| Ucx01000 | Kernel Driver | Manual | True | Running |
| UdeCx | Kernel Driver | Manual | False | Stopped |
| udfs | File System Driver | Disabled | True | Running |
| UEFI | Kernel Driver | Manual | False | Stopped |
| UevAgentDriver | File System Driver | Disabled | False | Stopped |
| Ufx01000 | Kernel Driver | Manual | False | Stopped |
| UfxChipidea | Kernel Driver | Manual | False | Stopped |
| ufxsynopsys | Kernel Driver | Manual | False | Stopped |
| umbus | Kernel Driver | Manual | True | Running |
| UmPass | Kernel Driver | Manual | False | Stopped |
| UrsChipidea | Kernel Driver | Manual | True | Running |
| UrsCx01000 | Kernel Driver | Manual | True | Running |
| UrsSynopsys | Kernel Driver | Manual | False | Stopped |
| usbaudio | Kernel Driver | Manual | False | Stopped |
| usbaudio2 | Kernel Driver | Manual | False | Stopped |
| usbccgp | Kernel Driver | Manual | True | Running |
| usbcir | Kernel Driver | Manual | False | Stopped |
| usbehci | Kernel Driver | Manual | True | Running |
| usbhub | Kernel Driver | Manual | True | Running |
| USBHUB3 | Kernel Driver | Manual | True | Running |
| usbohci | Kernel Driver | Manual | False | Stopped |
| usbprint | Kernel Driver | Manual | False | Stopped |
| usbser | Kernel Driver | Manual | False | Stopped |
| USBSTOR | Kernel Driver | Manual | True | Running |
| usbuhci | Kernel Driver | Manual | False | Stopped |
| USBXHCI | Kernel Driver | Manual | True | Running |
| vdrvroot | Kernel Driver | Boot | True | Running |
| VerifierExt | Kernel Driver | Disabled | False | Stopped |
| vhdmp | Kernel Driver | Manual | False | Stopped |
| vhf | Kernel Driver | Manual | False | Stopped |
| Vid | Kernel Driver | System | True | Running |
| VirtualRender | Kernel Driver | Manual | False | Stopped |
| vmbus | Kernel Driver | Boot | True | Running |
| VMBusHID | Kernel Driver | Manual | True | Running |
| vmgid | Kernel Driver | Manual | True | Running |
| volmgr | Kernel Driver | Boot | True | Running |
| volmgrx | Kernel Driver | Boot | True | Running |
| volsnap | Kernel Driver | Boot | True | Running |
| volume | Kernel Driver | Boot | True | Running |
| vpci | Kernel Driver | Manual | False | Stopped |
| vsmraid | Kernel Driver | Manual | False | Stopped |
| VSTXRAID | Kernel Driver | Manual | False | Stopped |
| vwifibus | Kernel Driver | Manual | False | Stopped |
| vwififlt | Kernel Driver | System | True | Running |
| WacomPen | Kernel Driver | Manual | False | Stopped |
| wanarp | Kernel Driver | Manual | False | Stopped |
| wanarpv6 | Kernel Driver | Manual | False | Stopped |
| wcifs | File System Driver | Auto | True | Running |
| wcnfs | File System Driver | Manual | False | Stopped |
| WdBoot | Kernel Driver | Boot | False | Stopped |
| Wdf01000 | Kernel Driver | Boot | True | Running |
| WdFilter | File System Driver | Boot | True | Running |
| wdiwifi | Kernel Driver | Manual | False | Stopped |
| WdmCompanionFilter | Kernel Driver | Manual | False | Stopped |
| WdNisDrv | Kernel Driver | Manual | True | Running |
| WFPLWFS | Kernel Driver | Boot | True | Running |
| WIMMount | File System Driver | Manual | False | Stopped |
| WindowsTrustedRT | Kernel Driver | Boot | True | Running |
| WindowsTrustedRTProxy | Kernel Driver | Boot | True | Running |
| WinMad | Kernel Driver | Manual | False | Stopped |
| WinNat | Kernel Driver | Manual | False | Stopped |
| WINUSB | Kernel Driver | Manual | False | Stopped |
| WinVerbs | Kernel Driver | Manual | False | Stopped |
| WmiAcpi | Kernel Driver | Manual | False | Stopped |
| Wof | File System Driver | Boot | True | Running |
| WpdUpFltr | Kernel Driver | Manual | False | Stopped |
| ws2ifsl | Kernel Driver | Disabled | False | Stopped |
| WudfPf | Kernel Driver | Manual | False | Stopped |
| WUDFRd | Kernel Driver | Manual | True | Running |
| xboxgip | Kernel Driver | Manual | False | Stopped |
| xinputhid | Kernel Driver | Manual | False | Stopped |

Table 47: [WMI] System Drivers

# [WMI] PNP Entities

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

| Name | Class GUID | Device ID | Hardware ID |
| --- | --- | --- | --- |
|  |  | VMBUS\POWERDEVICE\POWERDEVICE0 | VMBUS\PowerDevice |
|  |  | HTREE\ROOT\0 |  |
| ACPI Module Device | {4d36e97d-e325-11ce-bfc1-08002be10318} | ACPI\ACPI0004\0 | ACPI\VEN\_ACPI&DEV\_0004 ACPI\ACPI0004 \*ACPI0004 |
| ACPI x64-based PC | {4d36e966-e325-11ce-bfc1-08002be10318} | ROOT\ACPI\_HAL\0000 | acpiapic |
| Advanced programmable interrupt controller | {4d36e97d-e325-11ce-bfc1-08002be10318} | ACPI\PNP0003\3&FDAC00F&0 | ACPI\VEN\_PNP&DEV\_0003 ACPI\PNP0003 \*PNP0003 |
| AMD Ryzen 5 PRO 3500U w/ Radeon Vega Mobile Gfx | {50127dc3-0f36-415e-a6cc-4cb3be910b65} | ACPI\AUTHENTICAMD\_-\_AMD64\_FAMILY\_23\_MODEL\_24\_-\_AMD\_RYZEN\_5\_PRO\_3500U\_W/\_RADEON\_VEGA\_MOBILE\_GFX\1 | ACPI\VEN\_ACPI&DEV\_0007 ACPI\AuthenticAMD\_-\_AMD64\_Family\_23\_Model\_24 \*AuthenticAMD\_-\_AMD64\_Family\_23\_Model\_24 ACPI\AuthenticAMD\_-\_AMD64\_Family\_23 \*AuthenticAMD\_-\_AMD64\_Family\_23 ACPI\AuthenticAMD\_-\_AMD64 \*AuthenticAMD\_-\_AMD64 |
| Charge Arbitration Driver | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\CAD\0000 | ROOT\CAD |
| Composite Bus Enumerator | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\COMPOSITEBUS\0000 | ROOT\CompositeBus |
| Fax | {1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc} | SWD\PRINTENUM\{18F6F942-FB1D-45CA-BA27-93DBBB110309} | PRINTENUM\microsoftmicrosoft\_s7d14 PRINTENUM\LocalPrintQueue microsoftmicrosoft\_s7d14 |
| Generic Non-PnP Monitor | {4d36e96e-e325-11ce-bfc1-08002be10318} | DISPLAY\DEFAULT\_MONITOR\1&1F0C3C2F&0&UID256 | MONITOR\Default\_Monitor |
| Generic PnP Monitor | {4d36e96e-e325-11ce-bfc1-08002be10318} | DISPLAY\MSH062E\6&1A097CD8&0&UID5527112 | MONITOR\MSH062E |
| HID-compliant mouse | {4d36e96f-e325-11ce-bfc1-08002be10318} | HID\{CFA8B69E-5B4A-4CC0-B98B-8BA1A1F3F95A}\6&1A8C06AF&0&0000 | HID\{cfa8b69e-5b4a-4cc0-b98b-8ba1a1f3f95a} HID\{58f75a6d-d949-4320-99e1-a2a2576d581c} HID\VID\_045E&UP:0001\_U:0002 HID\_DEVICE\_SYSTEM\_MOUSE HID\_DEVICE\_UP:0001\_U:0002 HID\_DEVICE |
| Microsoft AC Adapter | {72631e54-78a4-11d0-bcf7-00aa00b7b32a} | ACPI\ACPI0003\3&FDAC00F&0 | ACPI\VEN\_ACPI&DEV\_0003 ACPI\ACPI0003 \*ACPI0003 |
| Microsoft ACPI-Compliant Control Method Battery | {72631e54-78a4-11d0-bcf7-00aa00b7b32a} | ACPI\PNP0C0A\3&FDAC00F&0 | ACPI\VEN\_PNP&DEV\_0C0A ACPI\PNP0C0A \*PNP0C0A |
| Microsoft ACPI-Compliant System | {4d36e97d-e325-11ce-bfc1-08002be10318} | ACPI\_HAL\PNP0C08\0 | ACPI\_HAL\PNP0C08 \*PNP0C08 |
| Microsoft Basic Display Driver | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\BASICDISPLAY\0000 | ROOT\BasicDisplay |
| Microsoft Basic Render Driver | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\BASICRENDER\0000 | ROOT\BasicRender |
| Microsoft GS Wavetable Synth | {62f9c741-b25a-46ce-b54c-9bccce08b6f2} | SWD\MMDEVAPI\MICROSOFTGSWAVETABLESYNTH |  |
| Microsoft Hyper-V Activation Component | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{3375BAF4-9E15-4B30-B765-67ACB10D607B}\{4487B255-B88C-403F-BB51-D1F69CF17F87} | VMBUS\{3375baf4-9e15-4b30-b765-67acb10d607b} VMBUS\{4487b255-b88c-403f-bb51-d1f69cf17f87} |
| Microsoft Hyper-V Data Exchange | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{A9A0F4E7-5A45-4D96-B827-8A841E8C03E6}\{242FF919-07DB-4180-9C2E-B86CB68C8C55} | VMBUS\{a9a0f4e7-5a45-4d96-b827-8a841e8c03e6} VMBUS\{242ff919-07db-4180-9c2e-b86cb68c8c55} |
| Microsoft Hyper-V Dynamic Memory | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{525074DC-8985-46E2-8057-A307DC18A502}\{1ECCFD72-4B41-45EF-B73A-4A6E44C12924} | VMBUS\{525074dc-8985-46e2-8057-a307dc18a502} VMBUS\{1eccfd72-4b41-45ef-b73a-4a6e44c12924} |
| Microsoft Hyper-V Generation Counter | {4d36e97d-e325-11ce-bfc1-08002be10318} | ACPI\HYPER\_V\_GEN\_COUNTER\_V1\0 | ACPI\Hyper\_V\_Gen\_Counter\_V1 \*Hyper\_V\_Gen\_Counter\_V1 |
| Microsoft Hyper-V Guest Service Interface | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{34D14BE3-DEE4-41C8-9AE7-6B174977C192}\{EB765408-105F-49B6-B4AA-C123B64D17D4} | VMBUS\{34d14be3-dee4-41c8-9ae7-6b174977c192} VMBUS\{eb765408-105f-49b6-b4aa-c123b64d17d4} |
| Microsoft Hyper-V Guest Shutdown | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{0E0B6031-5213-4934-818B-38D90CED39DB}\{B6650FF7-33BC-4840-8048-E0676786F393} | VMBUS\{0e0b6031-5213-4934-818b-38d90ced39db} VMBUS\{b6650ff7-33bc-4840-8048-e0676786f393} |
| Microsoft Hyper-V Heartbeat | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{57164F39-9115-4E78-AB55-382F3BD5422D}\{FD149E91-82E0-4A7D-AFA6-2A4166CBD7C0} | VMBUS\{57164f39-9115-4e78-ab55-382f3bd5422d} VMBUS\{fd149e91-82e0-4a7d-afa6-2a4166cbd7c0} |
| Microsoft Hyper-V Input | {745a17a0-74d3-11d0-b6fe-00a0c90f57da} | VMBUS\{CFA8B69E-5B4A-4CC0-B98B-8BA1A1F3F95A}\{58F75A6D-D949-4320-99E1-A2A2576D581C} | VMBUS\{cfa8b69e-5b4a-4cc0-b98b-8ba1a1f3f95a} VMBUS\{58f75a6d-d949-4320-99e1-a2a2576d581c} |
| Microsoft Hyper-V Network Adapter | {4d36e972-e325-11ce-bfc1-08002be10318} | VMBUS\{F8615163-DF3E-46C5-913F-F2D2F965ED0E}\{CE618ED8-802D-4843-8C45-AF6B13AC0608} | VMBUS\{f8615163-df3e-46c5-913f-f2d2f965ed0e} VMBUS\{ce618ed8-802d-4843-8c45-af6b13ac0608} |
| Microsoft Hyper-V Remote Desktop Control Channel | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{F8E65716-3CB3-4A06-9A60-1889C5CCCAB5}\{99221FA0-24AD-11E2-BE98-001AA01BBF6E} | VMBUS\{f8e65716-3cb3-4a06-9a60-1889c5cccab5} VMBUS\{99221fa0-24ad-11e2-be98-001aa01bbf6e} |
| Microsoft Hyper-V Remote Desktop Data Channel | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{F9E9C0D3-B511-4A48-8046-D38079A8830C}\{99221FA4-24AD-11E2-BE98-001AA01BBF6E} | VMBUS\{f9e9c0d3-b511-4a48-8046-d38079a8830c} VMBUS\{99221fa4-24ad-11e2-be98-001aa01bbf6e} |
| Microsoft Hyper-V Remote Desktop Virtualization | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{276AACF4-AC15-426C-98DD-7521AD3F01FE}\{F5BEE29C-1741-4AAD-A4C2-8FDEDB46DCC2} | VMBUS\{276aacf4-ac15-426c-98dd-7521ad3f01fe} VMBUS\{f5bee29c-1741-4aad-a4c2-8fdedb46dcc2} |
| Microsoft Hyper-V SCSI Controller | {4d36e97b-e325-11ce-bfc1-08002be10318} | VMBUS\{BA6163D9-04A1-4D29-B605-72E2FFB1DC7F}\{1A9656DE-9A41-43E6-B37F-AE375FD12A4A} | VMBUS\{ba6163d9-04a1-4d29-b605-72e2ffb1dc7f} VMBUS\{1a9656de-9a41-43e6-b37f-ae375fd12a4a} |
| Microsoft Hyper-V Time Synchronization | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{9527E630-D0AE-497B-ADCE-E80AB0175CAF}\{2DD1CE17-079E-403C-B352-A1921EE207EE} | VMBUS\{9527e630-d0ae-497b-adce-e80ab0175caf} VMBUS\{2dd1ce17-079e-403c-b352-a1921ee207ee} |
| Microsoft Hyper-V Video | {4d36e968-e325-11ce-bfc1-08002be10318} | VMBUS\{DA0A7802-E377-4AAC-8E77-0558EB1073F8}\{5620E0C7-8062-4DCE-AEB7-520C7EF76171} | VMBUS\{da0a7802-e377-4aac-8e77-0558eb1073f8} VMBUS\{5620e0c7-8062-4dce-aeb7-520c7ef76171} |
| Microsoft Hyper-V Virtual Keyboard | {4d36e96b-e325-11ce-bfc1-08002be10318} | VMBUS\{F912AD6D-2B17-48EA-BD65-F927A61C7684}\{D34B2567-B9B6-42B9-8778-0A4EC0B955BF} | VMBUS\{f912ad6d-2b17-48ea-bd65-f927a61c7684} VMBUS\{d34b2567-b9b6-42b9-8778-0a4ec0b955bf} |
| Microsoft Hyper-V Virtual Machine Bus | {4d36e97d-e325-11ce-bfc1-08002be10318} | ACPI\VMBUS\0 | ACPI\VMBus \*VMBus |
| Microsoft Hyper-V Virtualization Infrastructure Driver | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\VID\0000 | ROOT\VID |
| Microsoft Hyper-V Volume Shadow Copy | {4d36e97d-e325-11ce-bfc1-08002be10318} | VMBUS\{35FA2E29-EA23-4236-96AE-3A6EBACBA440}\{2450EE40-33BF-4FBD-892E-9FB06E9214CF} | VMBUS\{35fa2e29-ea23-4236-96ae-3a6ebacba440} VMBUS\{2450ee40-33bf-4fbd-892e-9fb06e9214cf} |
| Microsoft Kernel Debug Network Adapter | {4d36e972-e325-11ce-bfc1-08002be10318} | ROOT\KDNIC\0000 | root\kdnic |
| Microsoft Passport Container Enumeration Bus | {62f9c741-b25a-46ce-b54c-9bccce08b6f2} | SWD\SCDEVICEENUMBUS\1 |  |
| Microsoft Print to PDF | {1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc} | SWD\PRINTENUM\{C31F3C44-8549-4D02-BE1C-A03E3E25BB92} | PRINTENUM\{084f01fa-e634-4d77-83ee-074817c03581} PRINTENUM\LocalPrintQueue {084f01fa-e634-4d77-83ee-074817c03581} |
| Microsoft Radio Device Enumeration Bus | {62f9c741-b25a-46ce-b54c-9bccce08b6f2} | SWD\RADIO\{3DB5895D-CC28-44B3-AD3D-6F01A782B8D2} |  |
| Microsoft Remote Display Adapter | {4d36e968-e325-11ce-bfc1-08002be10318} | SWD\REMOTEDISPLAYENUM\RDPIDD\_INDIRECTDISPLAY&SESSIONID\_0002 | RdpIdd\_IndirectDisplay |
| Microsoft Storage Spaces Controller | {4d36e97b-e325-11ce-bfc1-08002be10318} | ROOT\SPACEPORT\0000 | Root\Spaceport |
| Microsoft System Management BIOS Driver | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\MSSMBIOS\0000 | ROOT\mssmbios |
| Microsoft Virtual Disk | {4d36e967-e325-11ce-bfc1-08002be10318} | SCSI\DISK&VEN\_MSFT&PROD\_VIRTUAL\_DISK\5&2C54316E&0&000000 | SCSI\DiskMsft\_\_\_\_Virtual\_Disk\_\_\_\_1.0\_ SCSI\DiskMsft\_\_\_\_Virtual\_Disk\_\_\_\_ SCSI\DiskMsft\_\_\_\_ SCSI\Msft\_\_\_\_Virtual\_Disk\_\_\_\_1 Msft\_\_\_\_Virtual\_Disk\_\_\_\_1 GenDisk |
| Microsoft Virtual Drive Enumerator | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\VDRVROOT\0000 | ROOT\vdrvroot |
| Microsoft Virtual DVD-ROM | {4d36e965-e325-11ce-bfc1-08002be10318} | SCSI\CDROM&VEN\_MSFT&PROD\_VIRTUAL\_DVD-ROM\5&2C54316E&0&000001 | SCSI\CdRomMsft\_\_\_\_Virtual\_DVD-ROM\_1.0\_ SCSI\CdRomMsft\_\_\_\_Virtual\_DVD-ROM\_ SCSI\CdRomMsft\_\_\_\_ SCSI\Msft\_\_\_\_Virtual\_DVD-ROM\_1 Msft\_\_\_\_Virtual\_DVD-ROM\_1 GenCdRom |
| Microsoft XPS Document Writer | {1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc} | SWD\PRINTENUM\{763BD821-10B3-4F5D-922D-CF1330E439B7} | PRINTENUM\{0f4130dd-19c7-7ab6-99a1-980f03b2ee4e} PRINTENUM\LocalPrintQueue {0f4130dd-19c7-7ab6-99a1-980f03b2ee4e} |
| NDIS Virtual Network Adapter Enumerator | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\NDISVIRTUALBUS\0000 | ROOT\NdisVirtualBus |
| OneNote | {1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc} | SWD\PRINTENUM\{0CB47077-B254-493F-97DF-B2DF15D3D49E} | PRINTENUM\{133619e4-143b-463a-b809-b1f51d05f973} PRINTENUM\LocalPrintQueue {133619e4-143b-463a-b809-b1f51d05f973} |
| Plug and Play Software Device Enumerator | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\SYSTEM\0000 | ROOT\SWENUM |
| Remote Audio | {c166523c-fe0c-4a94-a586-f1a80cfbbf3e} | SWD\MMDEVAPI\{3.0.0.00000002}.{6C26BA7D-F0B2-4225-B422-8168C5261E45} | MMDEVAPI\AudioEndpoints |
| Remote Desktop Camera Bus | {4d36e97d-e325-11ce-bfc1-08002be10318} | UMB\UMB\1&841921D&0&RDCAMERA\_BUS | UMB\UMBUS |
| Remote Desktop Device Redirector Bus | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\RDPBUS\0000 | ROOT\RDPBUS |
| Remote Desktop Keyboard Device | {4d36e96b-e325-11ce-bfc1-08002be10318} | TERMINPUT\_BUS\UMB\2&2C22BCC9&0&SESSION2KEYBOARD0 | TS\_INPT\TS\_KBD |
| Remote Desktop Mouse Device | {4d36e96f-e325-11ce-bfc1-08002be10318} | TERMINPUT\_BUS\UMB\2&2C22BCC9&0&SESSION2MOUSE0 | TS\_INPT\TS\_MOU |
| Remote Desktop USB Hub | {4d36e97d-e325-11ce-bfc1-08002be10318} | TS\_USB\_HUB\_ENUMERATOR\UMB\2&30D3618&0&TS\_USB\_HUB | UMB\TS\_URB\_HUB |
| Root Print Queue | {1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc} | SWD\PRINTENUM\PRINTQUEUES | PRINTENUM\LocalPrintQueue |
| Smart Card Device Enumeration Bus | {62f9c741-b25a-46ce-b54c-9bccce08b6f2} | SWD\SCDEVICEENUMBUS\0 |  |
| System CMOS/real time clock | {4d36e97d-e325-11ce-bfc1-08002be10318} | ACPI\PNP0B00\0 | ACPI\VEN\_PNP&DEV\_0B00 ACPI\PNP0B00 \*PNP0B00 |
| UMBus Enumerator | {4d36e97d-e325-11ce-bfc1-08002be10318} | UMB\UMB\1&841921D&0&TS\_USB\_HUB\_ENUMERATOR | UMB\UMBUS |
| UMBus Enumerator | {4d36e97d-e325-11ce-bfc1-08002be10318} | UMB\UMB\1&841921D&0&TERMINPUT\_BUS | UMB\UMBUS |
| UMBus Enumerator | {4d36e97d-e325-11ce-bfc1-08002be10318} | UMB\UMB\1&841921D&0&TSBUS | UMB\UMBUS |
| UMBus Root Bus Enumerator | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\UMBUS\0000 | root\umbus |
| Volume | {71a27cdd-812a-11d0-bec7-08002be2092f} | STORAGE\VOLUME\{23B589D8-2C14-11EB-94B4-806E6F6E6963}#0000000007500000 | STORAGE\Volume |
| Volume | {71a27cdd-812a-11d0-bec7-08002be2092f} | STORAGE\VOLUME\{23B589D8-2C14-11EB-94B4-806E6F6E6963}#0000000000100000 | STORAGE\Volume |
| Volume | {71a27cdd-812a-11d0-bec7-08002be2092f} | STORAGE\VOLUME\{23B589D8-2C14-11EB-94B4-806E6F6E6963}#0000000006500000 | STORAGE\Volume |
| Volume | {71a27cdd-812a-11d0-bec7-08002be2092f} | STORAGE\VOLUME\{23B589D8-2C14-11EB-94B4-806E6F6E6963}#0000000760500000 | STORAGE\Volume |
| Volume Manager | {4d36e97d-e325-11ce-bfc1-08002be10318} | ROOT\VOLMGR\0000 | ROOT\VOLMGR |

Table 48: [WMI] PNP Entities

# [System] Computer Certificates

This data is collected from the System.Security.Cryptography.X509Certificates.X509Store

## Basic

| 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 49: [System] Computer Certificates (Basic)

## Detailed

| Item | Value |
| --- | --- |
| ------ BLOCK 1 ------ | |
| Store | AuthRoot |
| Subject | DigiCert Global Root G2 |
| Issuer | DigiCert Global Root G2 |
| Valid From | 01/08/2013 13:00:00 |
| Expiration | 15/01/2038 12:00:00 |
| Thumbprint | DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 |
| Serial Number | 033AF1E6A711A9A0BB2864B11D09FAE5 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name | Server Authentication Client Authentication Secure Email Code Signing Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | DigiCert Global Root G2 |
| ------ BLOCK 2 ------ | |
| Store | AuthRoot |
| Subject | Baltimore CyberTrust Root |
| Issuer | Baltimore CyberTrust Root |
| Valid From | 12/05/2000 19:46:00 |
| Expiration | 13/05/2025 00:59:00 |
| Thumbprint | D4DE20D05E66FC53FE1A50882C78DB2852CAE474 |
| Serial Number | 020000B9 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha1RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.5 |
| Enhanced Key Usage List Friendly Name | Server Authentication Secure Email Client Authentication Code Signing OCSP Signing Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | DigiCert Baltimore Root |
| ------ BLOCK 3 ------ | |
| Store | AuthRoot |
| Subject | DigiCert Global Root CA |
| Issuer | DigiCert Global Root CA |
| Valid From | 10/11/2006 00:00:00 |
| Expiration | 10/11/2031 00:00:00 |
| Thumbprint | A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436 |
| Serial Number | 083BE056904246B1A1756AC95991C74A |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha1RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.5 |
| Enhanced Key Usage List Friendly Name | Server Authentication Client Authentication Secure Email Code Signing Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | DigiCert |
| ------ BLOCK 4 ------ | |
| Store | AuthRoot |
| Subject | Class 3 Public Primary Certification Authority |
| Issuer | Class 3 Public Primary Certification Authority |
| Valid From | 29/01/1996 00:00:00 |
| Expiration | 02/08/2028 00:59:59 |
| Thumbprint | 742C3192E607E424EB4549542BE1BBC53E6174E2 |
| Serial Number | 70BAE41D10D92934B638CA7B03CCBABF |
| Format | X509 |
| Version | 1 |
| Signature Algorithm Friendly Name | md2RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.2 |
| Enhanced Key Usage List Friendly Name | Secure Email Client Authentication Code Signing Server Authentication |
| Archived | False |
| Has Private Key | False |
| Friendly Name | VeriSign Class 3 Public Primary CA |
| ------ BLOCK 5 ------ | |
| Store | AuthRoot |
| Subject | Hotspot 2.0 Trust Root CA - 03 |
| Issuer | Hotspot 2.0 Trust Root CA - 03 |
| Valid From | 08/12/2013 12:00:00 |
| Expiration | 08/12/2043 12:00:00 |
| Thumbprint | 51501FBFCE69189D609CFAF140C576755DCC1FDF |
| Serial Number | 0CB30F70F286A433E0B90989DE01EDB7 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name | Server Authentication Client Authentication Secure Email |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Hotspot 2.0 Trust Root CA - 03 |
| ------ BLOCK 6 ------ | |
| Store | AuthRoot |
| Subject | Class 3 Public Primary Certification Authority |
| Issuer | Class 3 Public Primary Certification Authority |
| Valid From | 29/01/1996 00:00:00 |
| Expiration | 07/01/2004 23:59:59 |
| Thumbprint | 4F65566336DB6598581D584A596C87934D5F2AB4 |
| Serial Number | 00E49EFDF33AE80ECFA5113E19A4240232 |
| Format | X509 |
| Version | 1 |
| Signature Algorithm Friendly Name | md2RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.2 |
| Enhanced Key Usage List Friendly Name | Secure Email Client Authentication Code Signing Server Authentication |
| Archived | False |
| Has Private Key | False |
| Friendly Name | VeriSign Class 3 Primary CA |
| ------ BLOCK 7 ------ | |
| Store | CA |
| Subject | Root Agency |
| Issuer | Root Agency |
| Valid From | 28/05/1996 23:02:59 |
| Expiration | 31/12/2039 23:59:59 |
| Thumbprint | FEE449EE0E3965A5246F000E87FDE2A065FD89D4 |
| Serial Number | 06376C00AA00648A11CFB8D4AA5C35F4 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | md5RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.4 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 8 ------ | |
| Store | CA |
| Subject | www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign |
| Issuer | Class 3 Public Primary Certification Authority |
| Valid From | 17/04/1997 01:00:00 |
| Expiration | 25/10/2016 00:59:59 |
| Thumbprint | D559A586669B08F46A30A133F8A9ED3D038E2EA8 |
| Serial Number | 46FCEBBAB4D02F0F926098233F93078F |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha1RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.5 |
| Enhanced Key Usage List Friendly Name | Server Authentication Client Authentication |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 9 ------ | |
| Store | CA |
| Subject | Microsoft Windows Hardware Compatibility |
| Issuer | Microsoft Root Authority |
| Valid From | 01/10/1997 08:00:00 |
| Expiration | 31/12/2002 07:00:00 |
| Thumbprint | 109F1CAED645BB78B3EA2B94C0697C740733031C |
| Serial Number | 198B11D13F9A8FFE69A0 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | md5RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.4 |
| Enhanced Key Usage List Friendly Name | Code Signing Windows Hardware Driver Verification |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 10 ------ | |
| Store | eSIM Certification Authorities |
| Subject | GSM Association - RSP2 Root CI1 |
| Issuer | GSM Association - RSP2 Root CI1 |
| Valid From | 22/02/2017 00:00:00 |
| Expiration | 21/02/2052 23:59:59 |
| Thumbprint | D73F0C22273FA4C717A3A735F7E992F31190F010 |
| Serial Number | 6E68567A77A0EE7C85EE183963DFAA7A |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256ECDSA |
| Signature Algorithm Value | 1.2.840.10045.4.3.2 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 11 ------ | |
| Store | eSIM Certification Authorities |
| Subject | CMCA eSIM Root CA\_NIST |
| Issuer | CMCA eSIM Root CA\_NIST |
| Valid From | 05/09/2017 03:00:00 |
| Expiration | 05/09/2052 03:00:00 |
| Thumbprint | CE97FCF4ABACBFC662AF418EA1D4862F951D3D5D |
| Serial Number | 018B94 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256ECDSA |
| Signature Algorithm Value | 1.2.840.10045.4.3.2 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 12 ------ | |
| Store | eSIM Certification Authorities |
| Subject | China Unicom eSIM Root CA |
| Issuer | China Unicom eSIM Root CA |
| Valid From | 06/03/2017 17:00:00 |
| Expiration | 06/03/2037 17:00:00 |
| Thumbprint | 9E78FB9F9527D859700D303DFA589B3073951DCB |
| Serial Number | 0186F3 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256ECDSA |
| Signature Algorithm Value | 1.2.840.10045.4.3.2 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 13 ------ | |
| Store | FlightRoot |
| Subject | Microsoft Development Root Certificate Authority 2014 |
| Issuer | Microsoft Development Root Certificate Authority 2014 |
| Valid From | 28/05/2014 17:43:46 |
| Expiration | 28/05/2039 17:51:48 |
| Thumbprint | F8DB7E1C16F1FFD4AAAD4AAD8DFF0F2445184AEB |
| Serial Number | 078F0A9D03DF119E434E4FEC1BF0235A |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft Flighting Root 2014 |
| ------ BLOCK 14 ------ | |
| Store | FlightRoot |
| Subject | Microsoft ECC Development Root Certificate Authority 2018 |
| Issuer | Microsoft ECC Development Root Certificate Authority 2018 |
| Valid From | 27/02/2018 20:30:58 |
| Expiration | 27/02/2043 20:38:56 |
| Thumbprint | 6CA22E5501CC80885FF281DD8B3338E89398EE18 |
| Serial Number | 38623F7C7714C6AA4424574A882945AE |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha384ECDSA |
| Signature Algorithm Value | 1.2.840.10045.4.3.3 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft ECC Development Root Certificate Authority 2018 |
| ------ BLOCK 15 ------ | |
| Store | Remote Desktop |
| Subject | WS-01.ad.gr303.co.uk |
| Issuer | WS-01.ad.gr303.co.uk |
| Valid From | 20/11/2020 16:55:59 |
| Expiration | 22/05/2021 17:55:59 |
| Thumbprint | 34EF3E023141A3AD0E4CC4BC951B1B8FA9159D00 |
| Serial Number | 3A2CDB2994BB4D824D026DC3FF99C3D1 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name | Server Authentication |
| Archived | False |
| Has Private Key | True |
| Friendly Name |  |
| ------ BLOCK 16 ------ | |
| Store | ROOT |
| Subject | Microsoft Root Certificate Authority |
| Issuer | Microsoft Root Certificate Authority |
| Valid From | 10/05/2001 00:19:22 |
| Expiration | 10/05/2021 00:28:13 |
| Thumbprint | CDD4EEAE6000AC7F40C3802C171E30148030C072 |
| Serial Number | 79AD16A14AA0A5AD4C7358F407132E65 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha1RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.5 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft Root Certificate Authority |
| ------ BLOCK 17 ------ | |
| Store | ROOT |
| Subject | Thawte Timestamping CA |
| Issuer | Thawte Timestamping CA |
| Valid From | 01/01/1997 00:00:00 |
| Expiration | 31/12/2020 23:59:59 |
| Thumbprint | BE36A4562FB2EE05DBB3D32323ADF445084ED656 |
| Serial Number | 00 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | md5RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.4 |
| Enhanced Key Usage List Friendly Name | Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Thawte Timestamping CA |
| ------ BLOCK 18 ------ | |
| Store | ROOT |
| Subject | Microsoft Root Authority |
| Issuer | Microsoft Root Authority |
| Valid From | 10/01/1997 07:00:00 |
| Expiration | 31/12/2020 07:00:00 |
| Thumbprint | A43489159A520F0D93D032CCAF37E7FE20A8B419 |
| Serial Number | 00C1008B3C3C8811D13EF663ECDF40 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | md5RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.4 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft Root Authority |
| ------ BLOCK 19 ------ | |
| Store | ROOT |
| Subject | Symantec Enterprise Mobile Root for Microsoft |
| Issuer | Symantec Enterprise Mobile Root for Microsoft |
| Valid From | 15/03/2012 00:00:00 |
| Expiration | 14/03/2032 23:59:59 |
| Thumbprint | 92B46C76E13054E104F230517E6E504D43AB10B5 |
| Serial Number | 0F6B552F9EBF907B0F6629A9BDF4D8CE |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name | Code Signing |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 20 ------ | |
| Store | ROOT |
| Subject | Microsoft Root Certificate Authority 2011 |
| Issuer | Microsoft Root Certificate Authority 2011 |
| Valid From | 22/03/2011 22:05:28 |
| Expiration | 22/03/2036 22:13:04 |
| Thumbprint | 8F43288AD272F3103B6FB1428485EA3014C0BCFE |
| Serial Number | 3F8BC8B5FC9FB29643B569D66C42E144 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft Root Certificate Authority 2011 |
| ------ BLOCK 21 ------ | |
| Store | ROOT |
| Subject | Microsoft Authenticode(tm) Root Authority |
| Issuer | Microsoft Authenticode(tm) Root Authority |
| Valid From | 01/01/1995 08:00:01 |
| Expiration | 31/12/1999 23:59:59 |
| Thumbprint | 7F88CD7223F3C813818C994614A89C99FA3B5247 |
| Serial Number | 01 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | md5RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.4 |
| Enhanced Key Usage List Friendly Name | Secure Email Code Signing |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft Authenticode(tm) Root |
| ------ BLOCK 22 ------ | |
| Store | ROOT |
| Subject | Microsoft Root Certificate Authority 2010 |
| Issuer | Microsoft Root Certificate Authority 2010 |
| Valid From | 23/06/2010 22:57:24 |
| Expiration | 23/06/2035 23:04:01 |
| Thumbprint | 3B1EFD3A66EA28B16697394703A72CA340A05BD5 |
| Serial Number | 28CC3A25BFBA44AC449A9B586B4339AA |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft Root Certificate Authority 2010 |
| ------ BLOCK 23 ------ | |
| Store | ROOT |
| Subject | Microsoft ECC TS Root Certificate Authority 2018 |
| Issuer | Microsoft ECC TS Root Certificate Authority 2018 |
| Valid From | 27/02/2018 20:51:34 |
| Expiration | 27/02/2043 21:00:12 |
| Thumbprint | 31F9FC8BA3805986B721EA7295C65B3A44534274 |
| Serial Number | 153875E1647ED1B047B4EFAF41128245 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha384ECDSA |
| Signature Algorithm Value | 1.2.840.10045.4.3.3 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft ECC TS Root Certificate Authority 2018 |
| ------ BLOCK 24 ------ | |
| Store | ROOT |
| Subject | Copyright (c) 1997 Microsoft Corp. |
| Issuer | Copyright (c) 1997 Microsoft Corp. |
| Valid From | 13/05/1997 17:12:59 |
| Expiration | 30/12/1999 23:59:59 |
| Thumbprint | 245C97DF7514E7CF2DF8BE72AE957B9E04741E85 |
| Serial Number | 01 |
| Format | X509 |
| Version | 1 |
| Signature Algorithm Friendly Name | md5RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.4 |
| Enhanced Key Usage List Friendly Name | Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft Timestamp Root |
| ------ BLOCK 25 ------ | |
| Store | ROOT |
| Subject | NO LIABILITY ACCEPTED |
| Issuer | NO LIABILITY ACCEPTED |
| Valid From | 12/05/1997 01:00:00 |
| Expiration | 07/01/2004 23:59:59 |
| Thumbprint | 18F7C1FCC3090203FD5BAA2F861A754976C8DD25 |
| Serial Number | 4A19D2388C82591CA55D735F155DDCA3 |
| Format | X509 |
| Version | 1 |
| Signature Algorithm Friendly Name | md5RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.4 |
| Enhanced Key Usage List Friendly Name | Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | VeriSign Time Stamping CA |
| ------ BLOCK 26 ------ | |
| Store | ROOT |
| Subject | Microsoft ECC Product Root Certificate Authority 2018 |
| Issuer | Microsoft ECC Product Root Certificate Authority 2018 |
| Valid From | 27/02/2018 20:42:08 |
| Expiration | 27/02/2043 20:50:46 |
| Thumbprint | 06F1AA330B927B753A40E68CDF22E34BCBEF3352 |
| Serial Number | 14982666DC7CCD8F4053677BB999EC85 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha384ECDSA |
| Signature Algorithm Value | 1.2.840.10045.4.3.3 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft ECC Product Root Certificate Authority 2018 |
| ------ BLOCK 27 ------ | |
| Store | ROOT |
| Subject | Microsoft Time Stamp Root Certificate Authority 2014 |
| Issuer | Microsoft Time Stamp Root Certificate Authority 2014 |
| Valid From | 22/10/2014 23:08:57 |
| Expiration | 22/10/2039 23:15:19 |
| Thumbprint | 0119E81BE9A14CD8E22F40AC118C687ECBA3F4D8 |
| Serial Number | 2FD67A432293329045E953343EE27466 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft Time Stamp Root Certificate Authority 2014 |
| ------ BLOCK 28 ------ | |
| Store | ROOT |
| Subject | DigiCert Global Root G2 |
| Issuer | DigiCert Global Root G2 |
| Valid From | 01/08/2013 13:00:00 |
| Expiration | 15/01/2038 12:00:00 |
| Thumbprint | DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 |
| Serial Number | 033AF1E6A711A9A0BB2864B11D09FAE5 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name | Server Authentication Client Authentication Secure Email Code Signing Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | DigiCert Global Root G2 |
| ------ BLOCK 29 ------ | |
| Store | ROOT |
| Subject | Baltimore CyberTrust Root |
| Issuer | Baltimore CyberTrust Root |
| Valid From | 12/05/2000 19:46:00 |
| Expiration | 13/05/2025 00:59:00 |
| Thumbprint | D4DE20D05E66FC53FE1A50882C78DB2852CAE474 |
| Serial Number | 020000B9 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha1RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.5 |
| Enhanced Key Usage List Friendly Name | Server Authentication Secure Email Client Authentication Code Signing OCSP Signing Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | DigiCert Baltimore Root |
| ------ BLOCK 30 ------ | |
| Store | ROOT |
| Subject | DigiCert Global Root CA |
| Issuer | DigiCert Global Root CA |
| Valid From | 10/11/2006 00:00:00 |
| Expiration | 10/11/2031 00:00:00 |
| Thumbprint | A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436 |
| Serial Number | 083BE056904246B1A1756AC95991C74A |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha1RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.5 |
| Enhanced Key Usage List Friendly Name | Server Authentication Client Authentication Secure Email Code Signing Time Stamping |
| Archived | False |
| Has Private Key | False |
| Friendly Name | DigiCert |
| ------ BLOCK 31 ------ | |
| Store | ROOT |
| Subject | Class 3 Public Primary Certification Authority |
| Issuer | Class 3 Public Primary Certification Authority |
| Valid From | 29/01/1996 00:00:00 |
| Expiration | 02/08/2028 00:59:59 |
| Thumbprint | 742C3192E607E424EB4549542BE1BBC53E6174E2 |
| Serial Number | 70BAE41D10D92934B638CA7B03CCBABF |
| Format | X509 |
| Version | 1 |
| Signature Algorithm Friendly Name | md2RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.2 |
| Enhanced Key Usage List Friendly Name | Secure Email Client Authentication Code Signing Server Authentication |
| Archived | False |
| Has Private Key | False |
| Friendly Name | VeriSign Class 3 Public Primary CA |
| ------ BLOCK 32 ------ | |
| Store | ROOT |
| Subject | Hotspot 2.0 Trust Root CA - 03 |
| Issuer | Hotspot 2.0 Trust Root CA - 03 |
| Valid From | 08/12/2013 12:00:00 |
| Expiration | 08/12/2043 12:00:00 |
| Thumbprint | 51501FBFCE69189D609CFAF140C576755DCC1FDF |
| Serial Number | 0CB30F70F286A433E0B90989DE01EDB7 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name | Server Authentication Client Authentication Secure Email |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Hotspot 2.0 Trust Root CA - 03 |
| ------ BLOCK 33 ------ | |
| Store | ROOT |
| Subject | Class 3 Public Primary Certification Authority |
| Issuer | Class 3 Public Primary Certification Authority |
| Valid From | 29/01/1996 00:00:00 |
| Expiration | 07/01/2004 23:59:59 |
| Thumbprint | 4F65566336DB6598581D584A596C87934D5F2AB4 |
| Serial Number | 00E49EFDF33AE80ECFA5113E19A4240232 |
| Format | X509 |
| Version | 1 |
| Signature Algorithm Friendly Name | md2RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.2 |
| Enhanced Key Usage List Friendly Name | Secure Email Client Authentication Code Signing Server Authentication |
| Archived | False |
| Has Private Key | False |
| Friendly Name | VeriSign Class 3 Primary CA |
| ------ BLOCK 34 ------ | |
| Store | TestSignRoot |
| Subject | Microsoft ECC Testing Root Certificate Authority 2017 |
| Issuer | Microsoft ECC Testing Root Certificate Authority 2017 |
| Valid From | 09/11/2017 19:53:14 |
| Expiration | 09/11/2042 20:01:55 |
| Thumbprint | A4B37F4F6DE956922273D5CB8E7E0AAFB7033B90 |
| Serial Number | 6086A185EAFA2B9943B4671603F40323 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha384ECDSA |
| Signature Algorithm Value | 1.2.840.10045.4.3.3 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name | Microsoft ECC Testing Root Certificate Authority 2017 |
| ------ BLOCK 35 ------ | |
| Store | TestSignRoot |
| Subject | Microsoft Testing Root Certificate Authority 2010 |
| Issuer | Microsoft Testing Root Certificate Authority 2010 |
| Valid From | 17/06/2010 21:58:02 |
| Expiration | 17/06/2035 22:04:11 |
| Thumbprint | 8A334AA8052DD244A647306A76B8178FA215F344 |
| Serial Number | 7445C8784E0CC9964AB42FBCDA29E1BC |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 36 ------ | |
| Store | TestSignRoot |
| Subject | Microsoft Test Root Authority |
| Issuer | Microsoft Test Root Authority |
| Valid From | 10/01/1999 07:00:00 |
| Expiration | 31/12/2020 07:00:00 |
| Thumbprint | 2BD63D28D7BCD0E251195AEB519243C13142EBC3 |
| Serial Number | 5FEA4FD2F21D4310B6E8543ED8952618 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | md5RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.4 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 37 ------ | |
| Store | TrustedAppRoot |
| Subject | Microsoft VSMC PCA 2017 |
| Issuer | Microsoft Mobile Root Certificate Authority 2015 |
| Valid From | 26/09/2017 19:56:47 |
| Expiration | 26/09/2032 20:06:47 |
| Thumbprint | 11194FAB14616ED8259FB94DCD17CE99DAB04CDD |
| Serial Number | 33000000091DBA0349F054D5D3000000000009 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha256RSA |
| Signature Algorithm Value | 1.2.840.113549.1.1.11 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 38 ------ | |
| Store | Windows Live ID Token Issuer |
| Subject | Token Signing Public Key |
| Issuer | Token Signing Public Key |
| Valid From | 09/05/2016 21:40:55 |
| Expiration | 08/05/2021 21:40:55 |
| Thumbprint | 2C85006A1A028BCC349DF23C474724C055FDE8B6 |
| Serial Number | 00BEA900B78B6470EF |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha1DSA |
| Signature Algorithm Value | 1.2.840.10040.4.3 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |
| ------ BLOCK 39 ------ | |
| Store | Windows Live ID Token Issuer |
| Subject | Token Signing Public Key |
| Issuer | Token Signing Public Key |
| Valid From | 02/07/2013 22:10:37 |
| Expiration | 01/07/2018 22:10:37 |
| Thumbprint | 0217922CA1B6F0BD0F1D7FF6E7BDC29B2FAAA060 |
| Serial Number | 00BEBBCC34C2A99A43 |
| Format | X509 |
| Version | 3 |
| Signature Algorithm Friendly Name | sha1DSA |
| Signature Algorithm Value | 1.2.840.10040.4.3 |
| Enhanced Key Usage List Friendly Name |  |
| Archived | False |
| Has Private Key | False |
| Friendly Name |  |

Table 50: [System] Computer Certificates (Detailed)