Windows Machine Report

XCS-2K25-DEMO

Company Confidential

Date	Friday, February 14, 2025 3:55:51 PM
Author	CONTOSO\sysadmin
Version	1.11
Product	XIA Configuration Server [17.0.5.0]

Table of Contents

Disclaimer

Configuration Item

Provides general information for this item.

General Information

Name	XCS-2K25-DEMO
Description	Windows Server 2025 server running XIA Configuration Server.
Primary Owner Name	Technical Services
Primary Owner Contact	technicalservices@contosotravel.com

System Information

Item Path	Demonstration Company
Identifier	ec0a52da-1373-4068-b971-34700938513c
Item ID	1002
Version ID	1.11
Check Out Status	Available

VMware Virtual Platform

Custom Item Details

This is a demonstration Windows server running XIA Configuration Server.

Client Information

Provides information about the client that was used to generate the information and the data used by the client to uniquely identify this item.

Item Identifiers

Primary Identifier	XCS-2K25-DEMO
Secondary Identifier	VMware-56 4d 2f 76 0b 31 ee aa-7e 12 3b 54 62 da f1 74
Tertiary Identifier	
Environment Identifier	

Client Information

Client Machine Name	XCS-2K25-DEMO
Client Identifier	a5f92aec-9e9a-4d75-80d9-108e72daf65b
Client IP Address	192.168.128.6
Client Scan Date	14 February 2025 15:22 (today)
Client Service Username	CONTOSO\sysadmin
Client Version	17.0.5.0

Scan Profile

Target	XCS-2K25-DEMO
Profile Name	Windows
Profile Identifier	c4f3c375-1a3e-42ed-b303-d45a9ed5629a

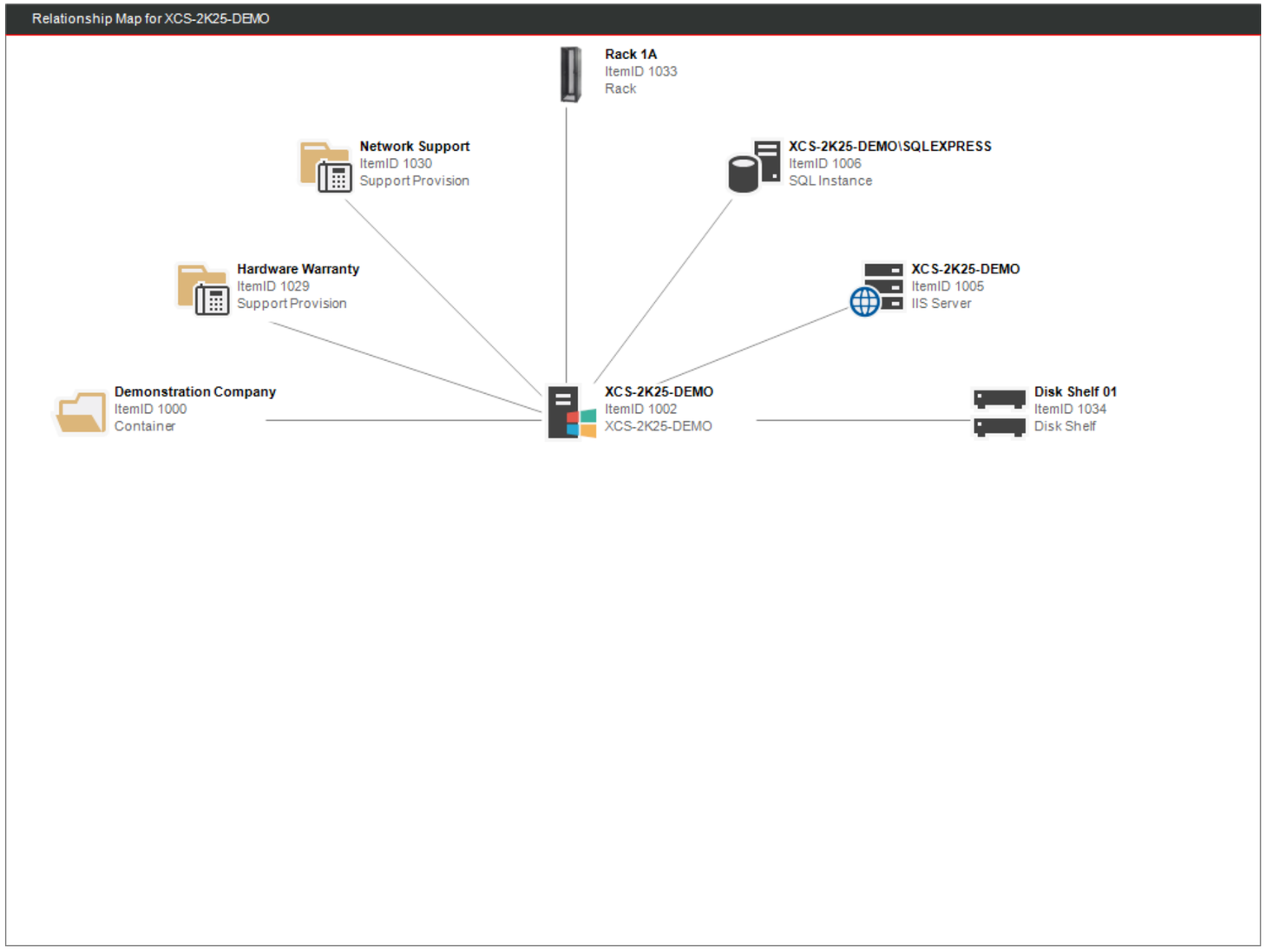
Relationships

Provides a summary of the relationships between this item and other items in the environment.

7 Relationships

Item ID	Direction	Name	Type	Relationship Type
1000	Outbound	Demonstration Company	Container	Contained Within
1029	Outbound	Hardware Warranty	Support Provision	Is Maintained By
1030	Outbound	Network Support	Support Provision	Is Supported By
1033	Outbound	Rack 1A	Rack	Located Within
1006	Outbound	XCS-2K25-DEMO\SQLEXPRESS	SQL Instance	Hosts SQL Instance
1005	Outbound	XCS-2K25-DEMO	IIS Server	Hosts IIS Server
1034	Outbound	Disk Shelf 01	Disk Shelf	Connected Disk Shelf

Relationship Map



Management Summary

Provides a management summary for this machine

Operating System

Operating System Name	Microsoft Windows Server 2025 Datacenter
Service Pack	[None Installed]

Naming and Role

Domain	contoso.com
Domain Role	Member Server
NetBIOS Name	XCS-2K25-DEMO
Fully Qualified Domain Name	xcs-2k25-demo.contoso.com

Hardware Information

Serial Number	VMware-56 4d 2f 76 0b 31 ee aa-7e 12 3b 54 62 da f1 74
Manufacturer	VMware, Inc.
Model	VMware20,1
Asset Tag	

Networking

IPv4 Addresses	192.168.128.6/22
IPv6 Addresses	fe80::8190:de8d:a907:7f94%7/0.0.0.64

Remote Desktop Settings

Allow Connections	False

Server Functions

Name	Enabled	Active	Instance Identifier
IIS Web Server	True	True	
SQL Instance	True	True	SQLEXPRESS

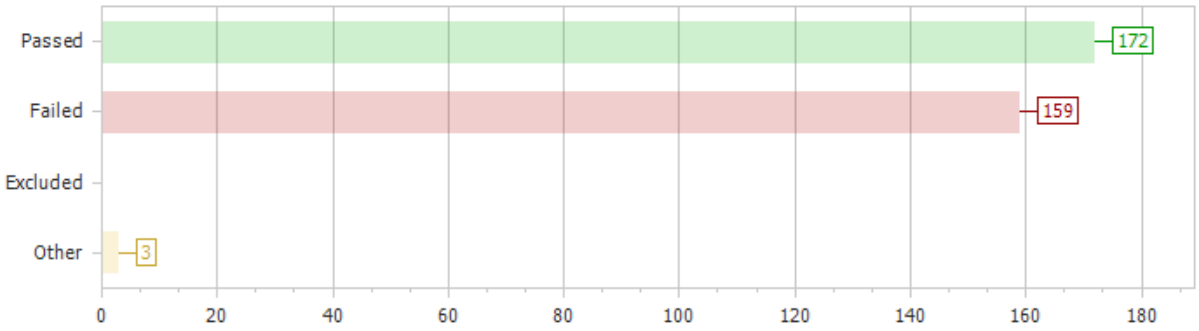
Compliance Benchmarks

Compliance benchmarks provide the ability to compare the documented configuration of an item against a known security or compliance baseline.

Name	Version	Passed	Failed	Other
Windows Basic Compliance Benchmark	5.0.0.0	172	159	3

Windows Basic Compliance Benchmark [5.0.0.0]

This benchmark provides a basic security overview of a Windows machine.



334 Benchmark Results

Ref.	Title	Configured Value
Section 1: Password Policy		
1.01	Set "Enforce password history" to remember at least 24 passwords	24
1.02	Set "Maximum password age" to 60 days or less	42 days
1.03	Set "Minimum password age" to at least 1 day(s)	1 days
1.04	Set "Minimum password length" to 14 or more characters	7
1.05	Set "Password must meet complexity requirements" to "Enabled"	Enabled
1.06	Set "Store passwords using reversible encryption" to "Disabled"	Disabled
1.07	Set "Relax minimum password length limits" to "Enabled" on supported operating systems	Not Configured
Section 2: Account Lockout Policy		
2.01	Set the "Account lockout duration" to 30 minutes or longer	Not Applicable
2.02	Set the "Account lockout threshold" to greater than 4 and less than 10	0
2.03	Set the "Reset account lockout counter after" value to between 15 minutes and 30 minutes	Not Applicable
Section 3: Windows Remote Management (WinRM)		
3.01	Set "Allow Basic Authentication" to "False" for the WinRM Client	True
3.02	Set "Allow Digest Authentication" to "False" for the WinRM Client	True
3.03	Set "Allow Unencrypted Traffic" to "False" for the WinRM Client	False
3.04	Set "Allow Basic Authentication" to "False" for the WinRM Service	False
3.05	Set "Allow Unencrypted Traffic" to "False" for the WinRM Service	False
3.06	Set "Disallow Storing RunAs Credentials" to "True" for the WinRM Service	False
3.07	Set "Allow Remote Shell Access" to "True" for the Windows Remote Shell	True
Section 4: Local Accounts		
4.01	Rename the local Administrator account to a less easily identifiable account name (does not apply to domain controllers)	Administrator

4.02	Set the local Administrator account to "Disabled" (does not apply to domain controllers)	Enabled
4.03	Rename the local Guest account to a less easily identifiable account name (does not apply to domain controllers)	Guest
4.04	Set the local Guest account to "Disabled" (does not apply to domain controllers)	True
Section 5: Server Functions		
5.01	Limit the number of server functions to one per server	IIS Web Server SQL Instance [SQLEXPRESS]
Section 6: Remote Desktop Settings		
6.01	Set "Connection Mode" to "Don't allow remote connections" or "Only allow connections with network level authentication (more secure)"	Don't allow remote connections
6.02	Set "Disable COM Port Redirection" to "True"	Don't allow remote connections
6.03	Set "Disable Drive Redirection" to "True"	Don't allow remote connections
6.04	Set "Disable LPT Port Redirection" to "True"	Don't allow remote connections
6.05	Set "Disable Plug and Play Device" to "True"	Don't allow remote connections
6.06	Set "Always Prompt For Password" to "True"	Don't allow remote connections
6.07	Set "Security Layer" to "SSL"	Don't allow remote connections
6.08	Set "Minimum Encryption Level" to "High"	Don't allow remote connections
6.09	Set "Single Session Restriction" to "True"	Don't allow remote connections
6.10	Set "Use Temporary Folders Per Session" to "True"	Don't allow remote connections
6.11	Set "Delete Temporary Folders On Exit" to "True"	Don't allow remote connections
6.12	Set "Require Secure RPC Communication" to "True"	Don't allow remote connections
Section 7: Audit Settings		
7.01	Set "Audit: Audit the access of global system objects" to "Disabled"	Disabled
7.02	Set "Audit: Audit the use of Backup and Restore privilege" to "Disabled"	Disabled
7.03	Set "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to "Enabled"	Not Defined
7.04	Set the "Audit Credential Validation" advanced audit policy to "Success and Failure"	Success
7.05	Set the "Audit Kerberos Authentication Service" advanced audit policy to "Success and Failure"	Success
7.06	Set the "Audit Kerberos Service Ticket Operations" advanced audit policy to "Success and Failure"	Success
7.07	Set the "Audit Other Account Logon Events" advanced audit policy to "Success and Failure"	None
7.08	Set the "Audit Application Group Management" advanced audit policy to "None"	None
7.09	Set the "Audit Computer Account Management" advanced audit policy to "Success and Failure"	Success
7.10	Set the "Audit Distribution Group Management" advanced audit policy to "None"	None
7.11	Set the "Audit Other Account Management Events" advanced audit policy to "Success and Failure"	None
7.12	Set the "Audit Security Group Management" advanced audit policy to "Success and Failure"	Success
7.13	Set the "Audit User Account Management" advanced audit policy to "Success and Failure"	Success
7.14	Set the "Audit DPAPI Activity" advanced audit policy to "Success and Failure"	None
7.15	Set the "Audit PNP Activity" advanced audit policy to "Any"	None

7.16	Set the "Audit Process Creation" advanced audit policy to "Success and Failure"	None
7.17	Set the "Audit Process Termination" advanced audit policy to "None"	None
7.18	Set the "Audit RPC Events" advanced audit policy to "None"	None
7.23	Set the "Audit Account Lockout" advanced audit policy to "Success"	Success
7.24	Set the "Audit Group Membership" advanced audit policy to "Success"	None
7.25	Set the "Audit IPsec Extended Mode" advanced audit policy to "None"	None
7.26	Set the "Audit IPsec Main Mode" advanced audit policy to "None"	None
7.27	Set the "Audit IPsec Quick Mode" advanced audit policy to "None"	None
7.28	Set the "Audit Logoff" advanced audit policy to "Success"	Success
7.29	Set the "Audit Logon" advanced audit policy to "Success and Failure"	Success and Failure
7.30	Set the "Audit Network Policy Server" advanced audit policy to "None"	Success and Failure
7.31	Set the "Audit Other Logon/Logoff Events" advanced audit policy to "None"	None
7.32	Set the "Audit Special Logon" advanced audit policy to "Success and Failure"	Success
7.33	Set the "Audit User/Device Claims" advanced audit policy to "None"	None
7.34	Set the "Audit Application Generated" advanced audit policy to "None"	None
7.35	Set the "Audit Central Access Policy Staging" advanced audit policy to "None"	None
7.36	Set the "Audit Certification Services" advanced audit policy to "None"	None
7.37	Set the "Audit Detailed File Share" advanced audit policy to "None"	None
7.38	Set the "Audit File Share" advanced audit policy to "None"	None
7.39	Set the "Audit File System" advanced audit policy to "None"	None
7.40	Set the "Audit Filtering Platform Connection" advanced audit policy to "None"	None
7.41	Set the "Audit Filtering Platform Packet Drop" advanced audit policy to "None"	None
7.42	Set the "Audit Handle Manipulation" advanced audit policy to "None"	None
7.43	Set the "Audit Kernel Object" advanced audit policy to "None"	None
7.44	Set the "Audit Other Object Access Events" advanced audit policy to "None"	None
7.45	Set the "Audit Registry" advanced audit policy to "None"	None
7.46	Set the "Audit Removable Storage" advanced audit policy to "None"	None
7.47	Set the "Audit SAM" advanced audit policy to "None"	None
7.48	Set the "Audit Audit Policy Change" advanced audit policy to "Success and Failure"	Success
7.49	Set the "Audit Authentication Policy Change" advanced audit policy to "Success and Failure"	Success
7.50	Set the "Audit Authorization Policy Change" advanced audit policy to "None"	None
7.51	Set the "Audit Filtering Platform Policy Change" advanced audit policy to "None"	None
7.52	Set the "Audit MPSSVC Rule-Level Policy Change" advanced audit policy to "Success"	None
7.53	Set the "Audit Other Policy Change Events" advanced audit policy to "None"	None
7.54	Set the "Audit Non Sensitive Privilege Use" advanced audit policy to "None"	None
7.55	Set the "Audit Other Privilege Use Events" advanced audit policy to "None"	None
7.56	Set the "Audit Sensitive Privilege Use" advanced audit policy to "None"	None
7.57	Set the "Audit IPsec Driver" advanced audit policy to "Success and Failure"	None

7.58	Set the "Audit Other System Events" advanced audit policy to "None"	Success and Failure
7.59	Set the "Audit Security State Change" advanced audit policy to "Success and Failure"	Success
7.60	Set the "Audit Security System Extension" advanced audit policy to "Success and Failure"	None
7.61	Set the "Audit System Integrity" advanced audit policy to "Success and Failure"	Success and Failure
Section 8: Windows Update		
8.01	Enable Windows Update to receive updates	Never check for updates (not recommended)
8.02	Configure Windows Update to use Windows Server Update Services (WSUS)	
Section 9: Windows Time		
9.01	Enable the Windows Time client on all machines	True
9.02	Set the NTP client type to "Domain Hierarchy (NT5DS)" for domain members and "NTP" for PDC emulators and machines on workgroups	Domain Hierarchy (NT5DS)
9.03	Enable the NTP server for domain controllers, and disable for all other servers and workstations	False
Section 10: SNMP		
10.01	If SNMP is enabled, ensure that no "public" or "private" SNMP community strings are configured	Not Installed
10.02	If SNMP is enabled, ensure that no writable SNMP community strings are configured	Not Installed
Section 11: Deprecated Components and Protocols		
11.01	Ensure that Server Message Block (SMB) version 1 is disabled for the server service	Server Feature Disabled
11.02	Ensure that Server Message Block (SMB) version 1 is disabled for the client	Disabled
Section 12: Windows Event Log		
12.01	Set the maximum size of the Application event log to 40,960 KB or greater	20,480 KB
12.02	Set the maximum size of the Security event log to 81,920 KB or greater	20,480 KB
12.03	Set the maximum size of the Setup event log to 20,480 KB or greater	1,028 KB
12.04	Set the maximum size of the System event log to 20,480 KB or greater	20,480 KB
12.05	Set the retention policy of the Application event log to 'Overwrite events as needed'	Overwrite events as needed
12.06	Set the retention policy of the Security event log to 'Overwrite events as needed'	Overwrite events as needed
12.07	Set the retention policy of the Setup event log to 'Overwrite events as needed'	Overwrite events as needed
12.08	Set the retention policy of the System event log to 'Overwrite events as needed'	Overwrite events as needed
Section 13: User Rights Assignment		
13.01	Set the "Access Credential Manager as a trusted caller" user right to [Empty]	
13.02	Set the "Access this computer from the network" user right to include only BUILTIN\Administrators NT AUTHORITY\Authenticated Users	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Users Everyone
13.03	Set the "Act as part of the operating system" user right to [Empty]	
13.05	Set the "Adjust memory quotas for a process" user right to include only BUILTIN\Administrators IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\MSSQL% NT SERVICE\SQLAgent% NT SERVICE\SQLSERVERAGENT	BUILTIN\Administrators IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXP

		RESS
13.06	Set the "Allow log on locally" user right to include only BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Users	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Users
13.07	Set the "Allow log on through Remote Desktop Services" user right to include only BUILTIN\Administrators BUILTIN\Remote Desktop Users	BUILTIN\Administrators BUILTIN\Remote Desktop Users
13.08	Set the "Back up files and directories" user right to include only BUILTIN\Administrators BUILTIN\Backup Operators	BUILTIN\Administrators BUILTIN\Backup Operators
13.09	Set the "Bypass traverse checking" user right to [Any Value]	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Users Everyone NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS
13.10	Set the "Change the system time" user right to include only BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE
13.11	Set the "Change the time zone" user right to [Any Value]	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE
13.12	Set the "Create a pagefile" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.13	Set the "Create a token object" user right to [Empty]	
13.14	Set the "Create global objects" user right to include only BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE
13.15	Set the "Create permanent shared objects" user right to [Empty]	
13.16	Set the "Create symbolic links" user right to include only BUILTIN\Administrators NT VIRTUAL MACHINE\Virtual Machines	BUILTIN\Administrators
13.17	Set the "Debug programs" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.18	Set the "Deny access to this computer from the network" user right to must include BUILTIN\Guests	
13.19	Set the "Deny log on as a batch job" user right to must include BUILTIN\Guests	
13.20	Set the "Deny log on as a service" user right to must include BUILTIN\Guests	
13.21	Set the "Deny log on locally" user right to must include BUILTIN\Guests	
13.22	Set the "Deny log on through Remote Desktop Services" user right to must include BUILTIN\Guests	
13.23	Set the "Enable computer and user accounts to be trusted for delegation" user right to [Empty]	
13.24	Set the "Force shutdown from a remote system" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.25	Set the "Generate security audits" user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\adfssrv NT SERVICE\drs	IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE

13.26	Set the "Impersonate a client after authentication" user right to include only BUILTIN\Administrators BUILTIN\IIS_IUSRS NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	BUILTIN\Administrators BUILTIN\IIS_IUSRS NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE S-1-5-99-216390572-1995538116-3857911515-2404958512-2623887229
13.27	Set the "Increase a process working set" user right to include only BUILTIN\Device Owners BUILTIN\Users Window Manager\Window Manager Group	BUILTIN\Users
13.28	Set the "Increase scheduling priority" user right to include only BUILTIN\Administrators Window Manager\Window Manager Group	BUILTIN\Administrators Window Manager\Window Manager Group
13.29	Set the "Load and unload device drivers" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.30	Set the "Lock pages in memory" user right to [Empty]	
13.31	Set the "Log on as a batch job" user right to include only BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\IIS_IUSRS BUILTIN\Performance Log Users	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\IIS_IUSRS BUILTIN\Performance Log Users
13.32	Set the "Log on as a service" user right to include only IIS APPPOOL\% NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	CONTOSO\sysadmin IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\NETWORK SERVICE NT SERVICE\ALL SERVICES NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS NT SERVICE\SQLTELEMETRY$SQLEXPRESS RESTRICTED SERVICES\ALL RESTRICTED SERVICES XCS-2K25-DEMO\SQLServer2005 SQLBrowserUser$XCS-2K25-DEMO XCS-2K25-DEMO\wu
13.33	Set the "Manage auditing and security log" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.34	Set the "Modify an object label" user right to [Empty]	
13.35	Set the "Modify firmware environment values" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.36	Set the "Obtain an impersonation token for another user in the same session" user right to include only BUILTIN\Administrators	Unknown
13.37	Set the "Perform volume maintenance tasks" user right to include only BUILTIN\Administrators	BUILTIN\Administrators NT SERVICE\MSSQL$SQLEXPRESS
13.38	Set the "Profile single process" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.39	Set the "Profile system performance" user right to include only BUILTIN\Administrators NT SERVICE\WdiServiceHost	BUILTIN\Administrators NT SERVICE\WdiServiceHost
13.40	Set the "Remove computer from docking station" user right to [Any Value]	BUILTIN\Administrators
13.41	Set the "Replace a process level token" user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE

		NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS
13.42	Set the "Restore files and directories" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Backup Operators
13.43	Set the "Shut down the system" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Backup Operators
13.44	Set the "Synchronize directory service data" user right to [Empty]	
13.45	Set the "Take ownership of files or other objects" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
Section 14: Windows Firewall Domain Profile		
14.01	Set the Windows Firewall domain profile firewall state to "On (recommended)"	On (recommended)
14.02	Set the Windows Firewall domain profile default inbound action to "Block (default)"	Block (default)
14.03	Set the Windows Firewall domain profile default outbound action to "Allow (default)"	Allow (default)
14.04	Set the Windows Firewall domain profile display a notification setting to "No"	No
14.05	Set the Windows Firewall domain profile excluded network interfaces to none	
14.06	Set the Windows Firewall domain profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\DomainProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
14.07	Set the Windows Firewall domain profile log file size limit to 16,384 KB or greater	4,096 KB
14.08	Set the Windows Firewall domain profile log dropped packets setting to "Yes"	No
14.09	Set the Windows Firewall domain profile log successful connections setting to "Yes"	No
Section 15: Windows Firewall Private Profile		
15.01	Set the Windows Firewall private profile firewall state to "On (recommended)"	On (recommended)
15.02	Set the Windows Firewall private profile default inbound action to "Block (default)"	Block (default)
15.03	Set the Windows Firewall private profile default outbound action to "Allow (default)"	Allow (default)
15.04	Set the Windows Firewall private profile display a notification setting to "No"	No
15.05	Set the Windows Firewall private profile excluded network interfaces to none	
15.06	Set the Windows Firewall private profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PrivateProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
15.07	Set the Windows Firewall private profile log file size limit to 16,384 KB or greater	4,096 KB
15.08	Set the Windows Firewall private profile log dropped packets setting to "Yes"	No
15.09	Set the Windows Firewall private profile log successful connections setting to "Yes"	No
Section 16: Windows Firewall Public Profile		
16.01	Set the Windows Firewall public profile firewall state to "On (recommended)"	On (recommended)
16.02	Set the Windows Firewall public profile default inbound action to "Block (default)"	Block (default)
16.03	Set the Windows Firewall public profile default outbound action to "Allow (default)"	Allow (default)
16.04	Set the Windows Firewall public profile display a notification setting to "No"	No
16.05	Set the Windows Firewall public profile excluded network interfaces to none	
16.06	Set the Windows Firewall public profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PublicProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
16.07	Set the Windows Firewall public profile log file size limit to 16,384 KB or greater	4,096 KB
16.08	Set the Windows Firewall public profile log dropped packets setting to "Yes"	No
16.09	Set the Windows Firewall public profile log successful connections setting to "Yes"	No

Section 17: Security Options (General)		
17.01	Set the "App Runtime: Allow Microsoft accounts to be optional" security option to "Enabled"	Not Defined
17.02	Set the "Biometrics: Configure enhanced anti-spoofing" security option to "Enabled"	Not Defined
17.03	Set the "Cloud Content: Turn off Microsoft consumer experiences" security option to "Enabled"	Not Defined
17.04	Set the "Connect: Require pin for pairing" security option to "First Time" or "Always"	Not Defined
17.05	Set the "OneDrive: Prevent the usage of OneDrive for file storage" security option to "Enabled"	Not Defined
17.06	Set the "Regional and Language Options: Allow users to enable online speech recognition services" security option to "Disabled"	Not Defined
17.07	Set the "Windows Ink Workspace: Allow Windows Ink Workspace" security option to "Disabled" or "On, but disallow access above lock"	Not Defined
Section 18: Security Options (Accounts)		
18.01	Set the "Accounts: Block Microsoft accounts" security option to "Users can’t add or log on with Microsoft accounts"	Not Defined
18.02	Set the "Accounts: Limit local account use of blank passwords to console logon only" security option to "Enabled"	Enabled
Section 19: Security Options (Audit)		
19.01	Set the "Audit Process Creation: Include command line in process creation events" security option to "Disabled" or "Not Defined"	Not Defined
19.02	Set the "Audit: Shut down system immediately if unable to log security audits" security option to "Disabled"	Disabled
Section 20: Security Options (Credential User Interface)		
20.01	Set the "Credential User Interface: Do not display the password reveal button" security option to "Enabled"	Not Defined
20.02	Set the "Credential User Interface: Enumerate administrator accounts on elevation" security option to "Disabled"	Not Defined
Section 21: Security Options (Credentials Delegation)		
21.01	Set the "Credentials Delegation: Encryption Oracle Remediation" security option to "Force Updated Clients"	Not Defined
21.02	Set the "Credentials Delegation: Remote host allows delegation of non-exportable credentials" security option to "Enabled"	Not Defined
Section 22: Security Options (Data Collection and Preview Builds)		
22.01	Set the "Data Collection and Preview Builds: Allow Diagnostics Data" security option to "Diagnostic data off (not recommended)" or "Send required diagnostic data" on Windows Server 2022, Windows 10 build 20348, Windows 11 and newer	Not Defined
22.03	Set the "Data Collection and Preview Builds: Do not show feedback notifications" security option to "Enabled"	Not Defined
22.04	Set the "Data Collection and Preview Builds: Toggle user control over Insider builds" security option to "Disabled"	Not Defined
Section 23: Security Options (Devices)		
23.01	Set the "Devices: Allowed to format and eject removable media" security option to "Administrators"	Not Defined
23.02	Set the "Devices: Prevent users from installing printer drivers" security option to "Enabled"	Enabled
Section 25: Security Options (Domain Members)		
25.01	Set the "Domain member: Digitally encrypt or sign secure channel data (always)" security option to "Enabled" on domain members	Enabled
25.02	Set the "Domain member: Digitally encrypt secure channel data (when possible)"	Enabled

	security option to "Enabled" on domain members	
25.03	Set the "Domain member: Digitally sign secure channel data (when possible)" security option to "Enabled" on domain members	Enabled
25.04	Set the "Domain member: Disable machine account password changes" security option to "Disabled" on domain members	Enabled
25.05	Set the "Domain member: Maximum machine account password age" security option to 30 days on domain members	30 days
25.06	Set the "Domain member: Require strong (Windows 2000 or later) session key" security option to "Enabled" on domain members	Enabled
Section 26: Security Options (Explorer Shell)		
26.01	Set the "AutoPlay Policies: Disallow Autoplay for non-volume devices" security option to "Enabled"	Not Defined
26.02	Set the "AutoPlay Policies: Set the default behavior for AutoRun" security option to "Do not execute any autorun commands"	Not Defined
26.03	Set the "AutoPlay Policies: Turn off Autoplay" security option to "All drives"	Not Defined
26.04	Set the "File Explorer: Configure Microsoft Defender SmartScreen" security option to "Warn and prevent bypass"	Not Defined
26.05	Set the "File Explorer: Enable Microsoft Defender SmartScreen" security option to "Enabled"	Not Defined
26.06	Set the "File Explorer: Turn off Data Execution Prevention for Explorer" security option to "Disabled"	Not Defined
26.07	Set the "File Explorer: Turn off heap termination on corruption" security option to "Disabled" or "Not Defined"	Not Defined
26.08	Set the "File Explorer: Turn off shell protocol protected mode" security option to "Disabled" or "Not Defined"	Not Defined
Section 27: Security Options (Group Policy)		
27.01	Set the "Group Policy: Continue experiences on this device" security option to "Disabled" on domain members	Not Defined
27.02	Set the "Group Policy: Registry policy processing: Do not apply during periodic background processing" security option to "Disabled" on domain members	Not Defined
27.03	Set the "Group Policy: Registry policy processing: Process even if the Group Policy objects have not changed" security option to "Enabled" on domain members	Not Defined
27.04	Set the "Group Policy: Turn off background refresh of Group Policy" security option to "Disabled" or "Not Defined" on domain members	Not Defined
Section 28: Security Options (Interactive Logon)		
28.01	Set the "Interactive logon: Don't display last signed-in" security option to "Enabled"	Disabled
28.02	Set the "Interactive logon: Do not require CTRL+ALT+DEL" security option to "Disabled"	Disabled
28.03	Set the "Interactive logon: Machine account lockout threshold" security option to a value between 6 and 10.	Not Defined
28.04	Set the "Interactive logon: Machine inactivity limit" security option to 900 seconds or less	Not Defined
28.05	Set the "Interactive logon: Message text for users attempting to log on" security option to an appropriate value	
28.06	Set the "Interactive logon: Message title for users attempting to log on" security option to an appropriate value	
28.07	Set the "Interactive logon: Number of previous logons to cache (in case domain controller is not available)" security option to "0" for servers and "0" for workstations on domain members that are not domain controllers	10 logons
28.08	Set the "Interactive logon: Prompt user to change password before expiration" security option to a value between 5 and 10 days	5 days
28.09	Set the "Interactive logon: Require Domain Controller authentication to unlock	Disabled

	workstation" security option to "Enabled" on domain members that are not domain controllers	
28.10	Set the "Interactive logon: Smart card removal behavior" security option to "Lock Workstation", "Force Logoff", or "Disconnect if a Remote Desktop Services session"	No Action
Section 29: Security Options (Internet Explorer - Deprecated)		
29.01	Set the "Internet Explorer: Disable Internet Explorer as a stand alone browser" security option to "Disable browser never notify user", "Disable browser always notify user", or "Disable browser notify user once"	Not Defined
29.02	Set the "Internet Explorer: Prevent downloading of enclosures" security option to "Enabled"	Not Defined
Section 30: Security Options (Lanman Workstation)		
30.01	Set the "Lanman Workstation: Enable insecure guest logons" security option to "Disabled"	Not Defined
Section 31: Security Options (Logon)		
31.01	Set the "Logon: Block user from showing account details on sign-in" security option to "Enabled"	Not Defined
31.02	Set the "Logon: Do not display network selection UI" security option to "Enabled"	Not Defined
31.03	Set the "Logon: Do not enumerate connected users on domain-joined computers" security option to "Enabled" on domain members	Not Defined
31.04	Set the "Logon: Enumerate local users on domain-joined computers" security option to "Disabled" on domain members that are not domain controllers	Not Defined
31.05	Set the "Logon: Turn off app notifications on the lock screen" security option to "Enabled"	Not Defined
31.06	Set the "Logon: Turn off picture password sign-in" security option to "Enabled" on domain members	Not Defined
31.07	Set the "Logon: Turn on convenience PIN sign-in" security option to "Disabled" on domain members	Not Defined
31.08	Set the "Windows Logon Options: Sign-in and lock last interactive user automatically after a restart" security setting to "Disabled"	Disabled
Section 32: Security Options (Microsoft Accounts)		
32.01	Set the "Microsoft Accounts: Block all consumer Microsoft account user authentication" security option to "Enabled"	Not Defined
Section 33: Security Options (Microsoft Defender Antivirus)		
33.01	Set the "Microsoft Defender Antivirus: Configure detection for potentially unwanted applications" security option to "Block"	Not Defined
33.02	Set the "Microsoft Defender Antivirus: Configure local setting override for reporting to Microsoft MAPS" security option to "Disabled" or "Not Defined"	Not Defined
33.03	Set the "Microsoft Defender Antivirus: Configure Watson events" security option to "Disabled"	Not Defined
33.04	Set the "Microsoft Defender Antivirus: Join Microsoft MAPS" security option to "Disabled" or "Not Defined"	Not Defined
33.05	Set the "Microsoft Defender Antivirus: Prevent users and apps from accessing dangerous websites" security option to "Block"	Not Defined
33.06	Set the "Microsoft Defender Antivirus: Scan removable drives" security option to "Enabled"	Not Defined
33.07	Set the "Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus" security option to "Disabled" or "Not Defined"	Enabled
33.08	Set the "Microsoft Defender Antivirus: Turn on behavior monitoring" security option to "Enabled" or "Not Defined"	Not Defined
33.09	Set the "Microsoft Defender Antivirus: Turn on e-mail scanning" security option to "Enabled"	Not Defined
Section 34: Security Options (Microsoft Network Client)		

34.01	Set the "Microsoft network client: Digitally sign communications (always)" security option to "Enabled"	Not Defined
34.02	Set the "Microsoft network client: Digitally sign communications (if server agrees)" security option to "Enabled"	Enabled
34.03	Set the "Microsoft network client: Send unencrypted password to connect to third-party SMB servers" security option to "Disabled"	Disabled
Section 35: Security Options (Microsoft Network Server)		
35.01	Set the "Microsoft network server: Amount of idle time required before suspending session" security option to "15 minutes"	15 minutes
35.02	Set the "Microsoft network server: Digitally sign communications (always)" security option to "Enabled"	Not Defined
35.03	Set the "Microsoft network server: Digitally sign communications (if client agrees)" security option to "Enabled"	Disabled
35.04	Set the "Microsoft network server: Disconnect clients when logon hours expire" security option to "Enabled"	Enabled
35.05	Set the "Microsoft network server: Server SPN target name validation level" security option to "Accept if provided by client" or "Required from client"	Not Defined
Section 36: Security Options (MSS - Deprecated)		
36.01	Set the "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)" security option to "Disabled" or "Not Defined"	Disabled
36.02	Set the "MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Not Defined
36.03	Set the "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Not Defined
36.04	Set the "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" security option to "Disabled"	Enabled
36.05	Set the "MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds" security option to "300000 or 5 minutes (recommended)"	Not Defined
36.06	Set the "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" security option to "Enabled"	Not Defined
36.07	Set the "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)" security option to "Disabled"	Not Defined
36.08	Set the "MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)" security option to "Enabled" or "Not Defined"	Not Defined
36.09	Set the "MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)" security option to 5 seconds or less	Not Defined
36.10	Set the "MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted" security option to 3	Not Defined
36.11	Set the "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted" security option to 3	Not Defined
36.12	Set the "MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning" security option to 90% or less	Not Defined
Section 37: Security Options (Network)		
37.01	Set the "DNS Client: Turn off multicast name resolution" security option to "Enabled"	Not Defined
37.02	Set the "TCP/IP: NetBT NodeType" security option to "P-node (recommended)"	Not Defined
Section 38: Security Options (Network Access)		
38.01	Set the "Network access: Allow anonymous SID/Name translation" security option to "Disabled" (must be set with Group Policy)	Disabled
38.02	Set the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" security option to "Enabled"	Disabled

38.03	Set the "Network access: Do not allow anonymous enumeration of SAM accounts" security option to "Enabled"	Enabled
38.04	Set the "Network access: Do not allow storage of passwords and credentials for network authentication" security option to "Enabled"	Disabled
38.05	Set the "Network access: Let Everyone permissions apply to anonymous users" security option to "Disabled"	Disabled
38.06	Set the "Network access: Named Pipes that can be accessed anonymously" security option to only contain [Empty]	
38.07	Set the "Network access: Remotely accessible registry paths and subpaths" security option to include only Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Perflib Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\SysmonLog	Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Perflib Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\SysmonLog
38.08	Set the "Network access: Remotely accessible registry paths" security option to include only Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications	Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications
38.09	Set the "Network access: Restrict anonymous access to Named Pipes and Shares" security option to "Enabled"	Enabled
38.10	Set the "Network access: Restrict clients allowed to make remote calls to SAM" security option to "Administrators: Remote Access: Allow" on stand-alone machines and domain members that are not domain controllers	Not Defined
38.11	Set the "Network access: Shares that can be accessed anonymously" security option to an empty value	Not Defined
38.12	Set the "Network access: Sharing and security model for local accounts" security option to "Classic - Local users authenticate as themselves"	Classic - local users authenticate as themselves
Section 39: Security Options (Network Connections)		
39.01	Set the "Network Connections: Prohibit installation and configuration of Network Bridge on your DNS domain network" security option to "Enabled"	Not Defined
39.02	Set the "Network Connections: Prohibit use of Internet Connection Sharing on your DNS domain network" security option to "Enabled"	Not Defined
39.03	Set the "Network Connections: Require domain users to elevate when setting a network's location" security option to "Enabled"	Not Defined
Section 40: Security Options (Network Provider)		
40.01	Set the "Network Provider: Hardened UNC Paths" security option to *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1	
Section 41: Security Options (Network Security)		
41.01	Set the "Network security: Allow Local System to use computer identity for NTLM" security option to "Enabled"	Not Defined
41.02	Set the "Network security: Allow LocalSystem NULL session fallback" security option to "Disabled"	Not Defined

41.03	Set the "Network security: Allow PKU2U authentication requests to this computer to use online identities" security option to "Disabled" on domain members	Not Defined
41.04	Set the "Network security: Configure encryption types allowed for Kerberos" security option to "AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types" on domain members	Not Defined
41.05	Set the "Network security: Do not store LAN Manager hash value on next password change" security option to "Enabled"	Enabled
41.06	Set the "Network security: Force logoff when logon hours expire" security option to "Enabled"	Disabled
41.07	Set the "Network security: LAN Manager authentication level" security option to "Send NTLMv2 response only. Refuse LM & NTLM"	Not Defined
41.08	Set the "Network security: LDAP client signing requirements" security option to "Require Signing"	Negotiate Signing
41.09	Set the "Network security: Minimum session security for NTLM SSP based (including secure RPC) clients" security option to "Require NTLMv2 session security, Require 128-bit encryption"	Require 128-bit encryption
41.10	Set the "Network security: Minimum session security for NTLM SSP based (including secure RPC) servers" security option to "Require NTLMv2 session security, Require 128-bit encryption"	Require 128-bit encryption
Section 42: Security Options (Personalization)		
42.01	Set the "Personalization: Prevent enabling lock screen camera" security option to "Enabled"	Not Defined
42.02	Set the "Personalization: Prevent enabling lock screen slide show" security option to "Enabled"	Not Defined
Section 43: Security Options (Recovery Console)		
43.01	Set the "Recovery console: Allow automatic administrative logon" security option to "Disabled"	Disabled
43.02	Set the "Recovery Console: Allow floppy copy and access to drives and folders" security option to "Disabled"	Disabled
Section 44: Security Options (Remote Assistance)		
44.01	Set the "Remote Assistance: Allow Offer Remote Assistance" security option to "Disabled"	Not Defined
44.02	Set the "Remote Assistance: Allow Solicited Remote Assistance" security option to "Disabled"	Not Defined
Section 45: Security Options (Remote Desktop Connection Client)		
45.01	Set the "Remote Desktop Connection Client: Do not allow passwords to be saved" security option to "Enabled"	Not Defined
Section 46: Security Options (Remote Procedure Call)		
46.01	Set the "Remote Procedure Call: Enable RPC Endpoint Mapper Client Authentication" security option to "Enabled" on domain members that are not domain controllers	Not Defined
46.02	Set the "Remote Procedure Call: Restrict Unauthenticated RPC clients" security option to "Authenticated" on domain members that are not domain controllers	Not Defined
Section 47: Security Options (Search)		
47.01	Set the "Search: Allow Cloud Search" security option to "Disable Cloud Search"	Not Defined
47.02	Set the "Search: Allow indexing of encrypted files" security option to "Disabled" or "Not Defined"	Not Defined
Section 48: Security Options (Security Providers)		
48.01	Set the "Security Providers: WDigest Authentication" security option to "Disabled" or "Not Defined"	Not Defined
Section 49: Security Options (Startup and Shutdown)		

49.01	Set the "Early Launch Antimalware: Boot-Start Driver Initialization Policy" security option to "Good, unknown and bad but critical" or "Not Defined"	Not Defined
49.02	Set the "Shutdown: Allow system to be shut down without having to log on" security option to "Disabled" (only applies to server operating systems)	Disabled
49.03	Set the "Shutdown: Clear virtual memory pagefile" security option to "Enabled"	Disabled
Section 50: Security Options (System Cryptography)		
50.01	Set the "System cryptography: Force strong key protection for user keys stored on the computer" security option to "User is prompted when the key is first used" or higher	Not Defined
Section 51: Security Options (System Objects)		
51.01	Set the "System objects: Require case insensitivity for non-Windows subsystems" security option to "Enabled"	Enabled
51.02	Set the "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)" security option to "Enabled"	Enabled
Section 52: Security Options (System Settings)		
52.01	Set the "System settings: Optional subsystems" security option to include only [Empty]	
52.02	Set the "System settings: Use certificate rules on Windows executables for Software Restriction Policies" security option to "Enabled"	Disabled
Section 53: Security Options (User Account Control)		
53.01	Set the "User Account Control: Admin Approval Mode for the Built-in Administrator account" security option to "Enabled"	Not Defined
53.02	Set the "User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop" security option to "Disabled"	Disabled
53.03	Set the "User Account Control: Apply UAC restrictions to local accounts on network logons" security option to "Enabled"	Not Defined
53.04	Set the "User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode" security option to "Prompt for consent on the secure desktop"	Prompt for consent for non-Windows binaries
53.05	Set the "User Account Control: Behavior of the elevation prompt for standard users" security option to "Automatically deny elevation requests"	Prompt for credentials
53.06	Set the "User Account Control: Detect application installations and prompt for elevation" security option to "Enabled"	Enabled
53.07	Set the "User Account Control: Only elevate UIAccess applications that are installed in secure locations" security option to "Enabled"	Enabled
53.08	Set the "User Account Control: Run all administrators in Admin Approval Mode" security option to "Enabled"	Enabled
53.09	Set the "User Account Control: Switch to the secure desktop when prompting for elevation" security option to "Enabled"	Enabled
53.10	Set the "User Account Control: Virtualize file and registry write failures to per-user locations" security option to "Enabled"	Enabled
Section 54: Security Options (Windows Connection Manager)		
54.01	Set the "Windows Connection Manager: Minimize the number of simultaneous connections to the Internet or a Windows Domain" security option to "1 = Minimize simultaneous connections" or "Not Defined"	Not Defined
54.02	Set the "Windows Connection Manager: Prohibit connection to non-domain networks when connected to domain authenticated network" security option to "Enabled" on domain members	Not Defined
Section 55: Security Options (Windows Installer)		
55.01	Set the "Windows Installer: Allow user control over installs" security option to "Disabled" or "Not Defined"	Not Defined
55.02	Set the "Windows Installer: Always install with elevated privileges" security option to "Disabled" or "Not Defined"	Not Defined

55.03	Set the "Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts'" security option to "Disabled" or "Not Defined"	Not Defined
Section 56: Security Options (Windows PowerShell)		
56.01	Set the "Windows PowerShell: Turn on PowerShell Script Block Logging" security option to "Enabled"	Not Defined
56.02	Set the "Windows PowerShell: Turn on PowerShell Transcription" security option to "Enabled"	Not Defined
Section 57: Security Options (Windows Security)		
57.01	Set the "Windows Security: App and browser protection: Prevent users from modifying settings" security option to "Enabled"	Not Defined

Location

Provides details of the physical location of this Windows machine.

UK

Street	Park Road
City	Oxford
State, Province, or County	Oxfordshire
ZIP or Postal Code	OX14 7AZ
Country	United Kingdom

Room

Name	DC Room 1

Rack

Name	Rack 1A

Hardware

This section provides a summary of the physical or virtual hardware present in the Windows machine.

Hardware Information

Serial Number	VMware-56 4d 2f 76 0b 31 ee aa-7e 12 3b 54 62 da f1 74
Manufacturer	VMware, Inc.
Model	VMware20,1
Asset Tag	

VMware Virtual Platform

Virtualization

Is Virtual Machine	True

Enclosure Details

Chassis Type	Other
Enclosure Serial Number	None
Enclosure Manufacturer	No Enclosure
Enclosure Model	

System Information

Motherboard Manufacturer	Intel Corporation
Motherboard	440BX Desktop Reference Platform
Processors Configuration	1 Processors
Total Physical Memory	4,095MB
UUID	762F4D56-310B-AAEE-7E12-3B5462DAF174

BIOS Information

Provides information about the basic input/output system of the Windows machine.

VMW201.00V.24006586.B64.2406042154

Manufacturer	VMware, Inc.
Release Date	Tuesday, June 4, 2024 1:00:00 AM
SMBIOS BIOS Version	VMW201.00V.24006586.B64.2406042154
Version	INTEL - 6040000
Current Language	
Embedded Controller Version	255.255.0.0
Firmware Type	UEFI
System BIOS Version	255.255.0.0

CD-ROM and DVD-ROM Drives

Provides details of the CD-ROM and DVD-ROM drives installed in the machine.

1 CD-ROM and DVD-ROM Drives

Drive ID	Name	Media Type	Manufacturer	Capabilities
D:	NECVMWar VMware SATA CD01	DVD-ROM	(Standard CD-ROM drives)	Random Access Supports Removable Media

Disk Drives

Provides information about the hard drives found in the Windows machine.

1 Disk Drives

Display Name	Interface	Serial Number	Partition Style	Size
[0] VMware Virtual NVMe Disk	NVMe	3635_B240_4D1F_BB3F_000C_2969_3BF8_8F0E.	GUID Partition Table (GPT)	60 GB

[0] VMware Virtual NVMe Disk

Provides information about the hard drives found in the Windows machine.

General

Model	VMware Virtual NVMe Disk
Firmware Revision	1.3
Bus Type	NVMe
Serial Number	3635_B240_4D1F_BB3F_000C_2969_3BF8_8F0E.
Size	60 GB
Location	nvme0
GUID	{3dc49ba1-98e9-4e70-aeda-82a958af2b17}
Capabilities	Random Access Supports Writing
Partition Style	GUID Partition Table (GPT)
Bytes Per Sector	512
Signature	
Sectors Per Track	63

Status

Operational Status	OK

Storage Pools

Storage Pool Names	Primordial

Unallocated Space

Unallocated Space	15 MB

3 Partitions

Identifier	Active	Type	Size
Disk #0, Partition #0	True	Other	100 MB
Disk #0, Partition #1	False	Basic (GPT)	59.23 GB
Disk #0, Partition #2	False	Other (GPT)	674 MB

C:

Active	False
Partition ID	Disk #0, Partition #1
Partition Type	Basic (GPT)
File System	NTFS
Volume Name	
Volume Serial Number	942A7DE1
Size	59.23 GB

C: (53% free)

Disk Shelves

Provides information about the disk shelves connected to this machine.

1 Connected Disk Shelves

Name	Manufacturer	Model	Product Number
Disk Shelf 01	Contoso Hardware	M04	PN005

Disk Shelf 01

Disk Shelf 01

Item ID	1034
Description	Description Windows servers disk shelf.
Primary Owner Name	Technical Services
Primary Owner Contact	technicalservices@contosotravel.com

Hardware Information

Serial Number	SN02
Manufacturer	Contoso Hardware
Model	M04
Asset Tag	AT04C
Product Number	PN005

Volumes

Provides information about the volumes found on this Windows machine.

3 Volumes

Name	Total Size	Free Space	Shadow Copy
C:	59.23 GB	31.52 GB	False
EFI System Partition (0276675f-8bbb-40fb-8dbc-1ca1cc906500)	96 MB	62.77 MB	False
Recovery Partition (e4f4a405-37f4-489c-88fc-3107f188d8fc)	674 MB	147.86 MB	False

C:

Provides information about the volumes found on this Windows machine.

Volume Details

Block Size	4,096
Capacity	59.23 GB
Drive Letter	C:
File System	NTFS
Label	
Volume Identifier	923e7279-c0c1-4f41-8f52-27ef1fd50898
Used Space	27.71 GB
Free Space	31.52 GB

Shadow Copy Configuration

Enabled	False

Disk Quota

State	Disabled

Security

Owner	NT SERVICE\TrustedInstaller

7 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
BUILTIN\Administrators	False	Allow	Full control	This folder, subfolders and files
BUILTIN\Users	False	Allow	Read & execute	This folder, subfolders and files
BUILTIN\Users	False	Allow	Create folders / append data	This folder and subfolders
BUILTIN\Users	False	Allow	Create files / write data	Subfolders only
CREATOR OWNER	False	Allow	Full control	Subfolders and files only
NT AUTHORITY\SYSTEM	False	Allow	Full control	This folder, subfolders and files
S-1-15-3-65536-1888954469-739942743-1668119174-2468466756-4239452838-1296943325-355587736-700089176	False	Allow	List folder / read data Read attributes Traverse folder / execute file	This folder or file only

0 NTFS Audit Rules

There are no audit rules found.

EFI System Partition (0276675f-8bbb-40fb-8dbc-1ca1cc906500)

Provides information about the volumes found on this Windows machine.

Volume Details

Block Size	1,024
Capacity	96 MB
Drive Letter	
File System	FAT32
Label	
Volume Identifier	0276675f-8bbb-40fb-8dbc-1ca1cc906500
Used Space	33.23 MB
Free Space	62.77 MB

Shadow Copy Configuration

Enabled	False

Recovery Partition (e4f4a405-37f4-489c-88fc-3107f188d8fc)

Provides information about the volumes found on this Windows machine.

Volume Details

Block Size	4,096
Capacity	674 MB
Drive Letter	
File System	NTFS
Label	
Volume Identifier	e4f4a405-37f4-489c-88fc-3107f188d8fc
Used Space	526.13 MB
Free Space	147.86 MB

Shadow Copy Configuration

Enabled	False

Devices

Provides details about the devices and drivers on this machine.

Audio inputs and outputs

Name	Driver Provider	Driver Version	Status
Microphone (High Definition Audio Device)	Microsoft	10.0.26100.1	Device is working properly.
Speakers (High Definition Audio Device)	Microsoft	10.0.26100.1	Device is working properly.

Batteries

Name	Driver Provider	Driver Version	Status
Microsoft AC Adapter	Microsoft	10.0.26100.3037	Device is working properly.

Computer

Name	Driver Provider	Driver Version	Status
ACPI x64-based PC	Microsoft	10.0.26100.1	Device is working properly.
VMware, Inc. VMware20,1	Microsoft	10.0.26100.1	Device is working properly.

Disk drives

Name	Driver Provider	Driver Version	Status
VMware Virtual NVMe Disk	Microsoft	10.0.26100.1150	Device is working properly.

Display adapters

Name	Driver Provider	Driver Version	Status
VMware SVGA 3D	VMware, Inc.	9.17.7.4	Device is working properly.

DVD/CD-ROM drives

Name	Driver Provider	Driver Version	Status
NECVMWar VMware SATA CD01	Microsoft	10.0.26100.1150	Device is working properly.

Human Interface Devices

Name	Driver Provider	Driver Version	Status
USB Input Device	Microsoft	10.0.26100.1882	Device is working properly.
USB Input Device	Microsoft	10.0.26100.1882	Device is working properly.

IDE ATA/ATAPI controllers

Name	Driver Provider	Driver Version	Status

ATA Channel 0	Microsoft	10.0.26100.1150	Device is working properly.
ATA Channel 1	Microsoft	10.0.26100.1150	Device is working properly.
Intel(R) 82371AB/EB PCI Bus Master IDE Controller	Microsoft	10.0.26100.1150	Device is working properly.
Standard SATA AHCI Controller	Microsoft	10.0.26100.1150	Device is working properly.

Keyboards

Name	Driver Provider	Driver Version	Status
Standard PS/2 Keyboard	Microsoft	10.0.26100.1882	Device is working properly.

Mice and other pointing devices

Name	Driver Provider	Driver Version	Status
VMware Pointing Device	VMware, Inc.	12.5.12.0	Device is working properly.
VMware USB Pointing Device	VMware, Inc.	12.5.12.0	Device is working properly.
VMware USB Pointing Device	VMware, Inc.	12.5.12.0	Device is working properly.

Monitors

Name	Driver Provider	Driver Version	Status
Generic Monitor	Microsoft	10.0.26100.1882	Device is working properly.

Network adapters

Name	Driver Provider	Driver Version	Status
Intel(R) 82574L Gigabit Network Connection	Microsoft	12.19.1.32	Device is working properly.
Microsoft Kernel Debug Network Adapter	Microsoft	10.0.26100.1150	Device is working properly.

Print queues

Name	Driver Provider	Driver Version	Status
Microsoft Print to PDF	Microsoft	10.0.26100.1	Device is working properly.
Root Print Queue	Microsoft	10.0.26100.1	Device is working properly.

Processors

Name	Driver Provider	Driver Version	Status
Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	Microsoft	10.0.26100.3037	Device is working properly.

Software devices

Name	Driver Provider	Driver Version	Status
Microsoft GS Wavetable Synth	Microsoft	10.0.26100.1	Device is working properly.
Microsoft Radio Device Enumeration Bus	Microsoft	10.0.26100.1	Device is working properly.

Sound, video and game controllers

Name	Driver Provider	Driver Version	Status
High Definition Audio Device	Microsoft	10.0.26100.1150	Device is working properly.

Storage controllers

Name	Driver Provider	Driver Version	Status
Microsoft Storage Spaces Controller	Microsoft	10.0.26100.3037	Device is working properly.
Standard NVM Express Controller	Microsoft	10.0.26100.3037	Device is working properly.

Storage volumes

Name	Driver Provider	Driver Version	Status
Volume	Microsoft	10.0.26100.1	Device is working properly.
Volume	Microsoft	10.0.26100.1	Device is working properly.
Volume	Microsoft	10.0.26100.1	Device is working properly.
Volume	Microsoft	10.0.26100.1	Device is working properly.

System devices

Name	Driver Provider	Driver Version	Status
ACPI Fixed Feature Button	Microsoft	10.0.26100.1150	Device is working properly.
Composite Bus Enumerator	Microsoft	10.0.26100.1150	Device is working properly.
CPU to PCI Bridge	Microsoft	10.0.26100.1150	Device is working properly.
Direct memory access controller	Microsoft	10.0.26100.1150	Device is working properly.
EISA programmable interrupt controller	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.

Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.

Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
Generic Bus	Microsoft	10.0.26100.1150	Device is working properly.
High Definition Audio Controller	Microsoft	10.0.26100.1882	Device is working properly.
High precision event timer	Microsoft	10.0.26100.1150	Device is working properly.
Microsoft ACPI-Compliant System	Microsoft	10.0.26100.3037	Device is working properly.
Microsoft Basic Display Driver	Microsoft	10.0.26100.1150	Device is working properly.
Microsoft Basic Render Driver	Microsoft	10.0.26100.1150	Device is working properly.
Microsoft Hyper-V Generation Counter	Microsoft	10.0.26100.1150	Device is working properly.
Microsoft System Management BIOS Driver	Microsoft	10.0.26100.1	Device is working properly.
Microsoft Virtual Drive Enumerator	Microsoft	10.0.26100.1591	Device is working properly.
Motherboard resources	Microsoft	10.0.26100.1150	Device is working properly.
Motherboard resources	Microsoft	10.0.26100.1150	Device is working properly.
NDIS Virtual Network Adapter Enumerator	Microsoft	10.0.26100.1	Device is working properly.
PCI Bus	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.

PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI Express Root Port	Microsoft	10.0.26100.3037	Device is working properly.
PCI to ISA Bridge	Microsoft	10.0.26100.1150	Device is working properly.
PCI-to-PCI Bridge	Microsoft	10.0.26100.3037	Device is working properly.
PCI-to-PCI Bridge	Microsoft	10.0.26100.3037	Device is working properly.
Plug and Play Software Device Enumerator	Microsoft	10.0.26100.1	Device is working properly.
Remote Desktop Device Redirector Bus	Microsoft	10.0.26100.1150	Device is working properly.
System CMOS/real time clock	Microsoft	10.0.26100.1150	Device is working properly.
System speaker	Microsoft	10.0.26100.1150	Device is working properly.
System timer	Microsoft	10.0.26100.1150	Device is working properly.
UMBus Root Bus Enumerator	Microsoft	10.0.26100.1150	Device is working properly.
VMware VMCI Bus Device	Broadcom Inc.	9.8.18.1	Device is working properly.
VMware VMCI Host Device	Broadcom Inc.	9.8.18.1	Device is working properly.
Volume Manager	Microsoft	10.0.26100.1150	Device is working properly.

Universal Serial Bus controllers

Name	Driver Provider	Driver Version	Status

Standard Enhanced PCI to USB Host Controller	Microsoft	10.0.26100.1882	Device is working properly.
Standard Universal PCI to USB Host Controller	Microsoft	10.0.26100.1882	Device is working properly.
Standard USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)	Microsoft	10.0.26100.3037	Device is working properly.
USB Composite Device	Microsoft	10.0.26100.1882	Device is working properly.
USB Root Hub	Microsoft	10.0.26100.1882	Device is working properly.
USB Root Hub	Microsoft	10.0.26100.1882	Device is working properly.
USB Root Hub (USB 3.0)	Microsoft	10.0.26100.3037	Device is working properly.

Audio inputs and outputs

Microphone (High Definition Audio Device)

Microphone (High Definition Audio Device)

Class	Audio inputs and outputs
Class GUID	{c166523c-fe0c-4a94-a586-f1a80cfbbf3e}
Device Status	Device is working properly.
PNP Device Identifier	SWD\MMDEVAPI\{0.0.1.00000000}.{06C654F9-9C9B-4D30-AE12-9BBC817E548E}
Manufacturer	Microsoft

Driver Details

Driver Date	Sunday, March 31, 2024
Device Class	AUDIOENDPOINT
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Friendly Name	Microphone (High Definition Audio Device)
Inf Name	audioendpoint.inf

Speakers (High Definition Audio Device)

Speakers (High Definition Audio Device)

Class	Audio inputs and outputs
Class GUID	{c166523c-fe0c-4a94-a586-f1a80cfbbf3e}
Device Status	Device is working properly.
PNP Device Identifier	SWD\MMDEVAPI\{0.0.0.00000000}.{C833DDDB-3A30-4D13-AABC-BD9E14F264AF}
Manufacturer	Microsoft

Driver Details

Driver Date	Sunday, March 31, 2024
Device Class	AUDIOENDPOINT
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Friendly Name	Speakers (High Definition Audio Device)
Inf Name	audioendpoint.inf

Batteries

Microsoft AC Adapter

Microsoft AC Adapter

Class	Batteries
Class GUID	{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\ACPI0003\1
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	BATTERY
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	cmbatt.inf

Computer

ACPI x64-based PC

ACPI x64-based PC

Class	Computer
Class GUID	{4d36e966-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\ACPI_HAL\0000
Manufacturer	(Standard computers)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	COMPUTER
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Inf Name	hal.inf

VMware, Inc. VMware20,1

VMware, Inc. VMware20,1

Class	Computer
Class GUID	{4d36e966-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	SWD\COMPUTER\MFG_VMWARE__INC.&PROD_VMWARE20_1
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	COMPUTER
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Friendly Name	VMware, Inc. VMware20,1
Inf Name	compdev.inf

Disk drives

VMware Virtual NVMe Disk

VMware Virtual NVMe Disk

Class	Disk drives
Class GUID	{4d36e967-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	SCSI\DISK&VEN_NVME&PROD_VMWARE_VIRTUAL_N\5&290F3806&0&000000
Manufacturer	(Standard disk drives)
Location	Bus Number 0, Target Id 0, LUN 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	DISKDRIVE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Friendly Name	VMware Virtual NVMe Disk
Inf Name	disk.inf

Display adapters

VMware SVGA 3D

VMware SVGA 3D

Class	Display adapters
Class GUID	{4d36e968-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_0405&SUBSYS_040515AD&REV_00\3&18D45AA6&0&78
Manufacturer	VMware, Inc.
Location	PCI bus 0, device 15, function 0

Driver Details

Driver Date	Tuesday, March 26, 2024
Device Class	DISPLAY
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	9.17.7.4
Inf Name	oem6.inf

DVD/CD-ROM drives

NECVMWar VMware SATA CD01

NECVMWar VMware SATA CD01

Class	DVD/CD-ROM drives
Class GUID	{4d36e965-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD01\5&36C0E7D6&0&010000
Manufacturer	(Standard CD-ROM drives)
Location	Bus Number 1, Target Id 0, LUN 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	CDROM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Friendly Name	NECVMWar VMware SATA CD01
Inf Name	cdrom.inf

Human Interface Devices

USB Input Device

USB Input Device

Class	Human Interface Devices
Class GUID	{745a17a0-74d3-11d0-b6fe-00a0c90f57da}
Device Status	Device is working properly.
PNP Device Identifier	USB\VID_0E0F&PID_0003&MI_00\7&4315E8A&0&0000
Manufacturer	(Standard system devices)
Location	000b.0000.0000.005.000.000.000.000.000

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	HIDCLASS
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	input.inf

USB Input Device

USB Input Device

Class	Human Interface Devices
Class GUID	{745a17a0-74d3-11d0-b6fe-00a0c90f57da}
Device Status	Device is working properly.
PNP Device Identifier	USB\VID_0E0F&PID_0003&MI_01\7&4315E8A&0&0001
Manufacturer	(Standard system devices)
Location	000b.0000.0000.005.000.000.000.000.000

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	HIDCLASS
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	input.inf

IDE ATA/ATAPI controllers

ATA Channel 0

ATA Channel 0

Class	IDE ATA/ATAPI controllers
Class GUID	{4d36e96a-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCIIDE\IDECHANNEL\4&39EC5D8A&0&0
Manufacturer	(Standard IDE ATA/ATAPI controllers)
Location	Channel 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	HDC
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Friendly Name	ATA Channel 0
Inf Name	mshdc.inf

ATA Channel 1

ATA Channel 1

Class	IDE ATA/ATAPI controllers
Class GUID	{4d36e96a-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCIIDE\IDECHANNEL\4&39EC5D8A&0&1
Manufacturer	(Standard IDE ATA/ATAPI controllers)
Location	Channel 1

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	HDC
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Friendly Name	ATA Channel 1
Inf Name	mshdc.inf

Intel(R) 82371AB/EB PCI Bus Master IDE Controller

Intel(R) 82371AB/EB PCI Bus Master IDE Controller

Class	IDE ATA/ATAPI controllers
Class GUID	{4d36e96a-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_8086&DEV_7111&SUBSYS_197615AD&REV_01\3&18D45AA6&0&39
Manufacturer	Intel
Location	PCI bus 0, device 7, function 1

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	HDC
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	mshdc.inf

Standard SATA AHCI Controller

Standard SATA AHCI Controller

Class	IDE ATA/ATAPI controllers
Class GUID	{4d36e96a-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07E0&SUBSYS_07E015AD&REV_00\4&B70F118&0&1888
Manufacturer	Standard SATA AHCI Controller
Location	PCI bus 2, device 3, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	HDC
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	mshdc.inf

Keyboards

Standard PS/2 Keyboard

Standard PS/2 Keyboard

Class	Keyboards
Class GUID	{4d36e96b-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0303\4&25EE97C0&0
Manufacturer	(Standard keyboards)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	KEYBOARD
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	keyboard.inf

Mice and other pointing devices

VMware Pointing Device

VMware Pointing Device

Class	Mice and other pointing devices
Class GUID	{4d36e96f-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\VMW0003\4&25EE97C0&0
Manufacturer	VMware, Inc.

Driver Details

Driver Date	Wednesday, October 27, 2021 1:00:00 AM
Device Class	MOUSE
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	12.5.12.0
Inf Name	oem5.inf

VMware USB Pointing Device

VMware USB Pointing Device

Class	Mice and other pointing devices
Class GUID	{4d36e96f-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	HID\VID_0E0F&PID_0003&MI_01\8&368F3BD5&0&0000
Manufacturer	VMware, Inc.

Driver Details

Driver Date	Wednesday, October 27, 2021 1:00:00 AM
Device Class	MOUSE
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	12.5.12.0
Inf Name	oem4.inf

VMware USB Pointing Device

VMware USB Pointing Device

Class	Mice and other pointing devices
Class GUID	{4d36e96f-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	HID\VID_0E0F&PID_0003&MI_00\8&235F1F97&0&0000
Manufacturer	VMware, Inc.

Driver Details

Driver Date	Wednesday, October 27, 2021 1:00:00 AM
Device Class	MOUSE
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	12.5.12.0
Inf Name	oem4.inf

Monitors

Generic Monitor

Generic Monitor

Class	Monitors
Class GUID	{4d36e96e-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	DISPLAY\DEFAULT_MONITOR\4&31BE19FA&0&UID0
Manufacturer	(Standard monitor types)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	MONITOR
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Friendly Name	Generic Monitor
Inf Name	monitor.inf

Network adapters

Intel(R) 82574L Gigabit Network Connection

Intel(R) 82574L Gigabit Network Connection

Class	Network adapters
Class GUID	{4d36e972-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_8086&DEV_10D3&SUBSYS_07D015AD&REV_00\000C29FFFFDAF17400
Manufacturer	Intel Corporation
Location	PCI bus 3, device 0, function 0

Driver Details

Driver Date	Sunday, March 8, 2015
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	12.19.1.32
Friendly Name	Intel(R) 82574L Gigabit Network Connection
Inf Name	net1ix64.inf

Microsoft Kernel Debug Network Adapter

Microsoft Kernel Debug Network Adapter

Class	Network adapters
Class GUID	{4d36e972-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\KDNIC\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Friendly Name	Microsoft Kernel Debug Network Adapter
Inf Name	kdnic.inf

Print queues

Microsoft Print to PDF

Microsoft Print to PDF

Class	Print queues
Class GUID	{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}
Device Status	Device is working properly.
PNP Device Identifier	SWD\PRINTENUM\{10DC8BBC-8CA6-4AC6-9892-4E20BD7CE340}
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	PRINTQUEUE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Friendly Name	Microsoft Print to PDF
Inf Name	printqueue.inf

Root Print Queue

Root Print Queue

Class	Print queues
Class GUID	{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}
Device Status	Device is working properly.
PNP Device Identifier	SWD\PRINTENUM\PRINTQUEUES
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	PRINTQUEUE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Friendly Name	Root Print Queue
Inf Name	printqueue.inf

Processors

Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz

Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz

Class	Processors
Class GUID	{50127dc3-0f36-415e-a6cc-4cb3be910b65}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_165_-_INTEL(R)_CORE(TM)_I9-10885H_CPU_@_2.40GHZ_0
Manufacturer	Intel

Driver Details

Driver Date	Tuesday, April 21, 2009 1:00:00 AM
Device Class	PROCESSOR
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Friendly Name	Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz
Inf Name	cpu.inf

Software devices

Microsoft GS Wavetable Synth

Microsoft GS Wavetable Synth

Class	Software devices
Class GUID	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}
Device Status	Device is working properly.
PNP Device Identifier	SWD\MMDEVAPI\MICROSOFTGSWAVETABLESYNTH
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SOFTWAREDEVICE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Friendly Name	Microsoft GS Wavetable Synth
Inf Name	c_swdevice.inf

Microsoft Radio Device Enumeration Bus

Microsoft Radio Device Enumeration Bus

Class	Software devices
Class GUID	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}
Device Status	Device is working properly.
PNP Device Identifier	SWD\RADIO\{3DB5895D-CC28-44B3-AD3D-6F01A782B8D2}
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SOFTWAREDEVICE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Friendly Name	Microsoft Radio Device Enumeration Bus
Inf Name	c_swdevice.inf

Sound, video and game controllers

High Definition Audio Device

High Definition Audio Device

Class	Sound, video and game controllers
Class GUID	{4d36e96c-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	HDAUDIO\FUNC_01&VEN_15AD&DEV_1975&SUBSYS_15AD1975&REV_1001\5&322E5E46&0&0001
Manufacturer	Microsoft
Location	Internal High Definition Audio Bus

Driver Details

Driver Date	Thursday, March 7, 2024
Device Class	MEDIA
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	hdaudio.inf

Storage controllers

Microsoft Storage Spaces Controller

Microsoft Storage Spaces Controller

Class	Storage controllers
Class GUID	{4d36e97b-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\SPACEPORT\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SCSIADAPTER
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	spaceport.inf

Standard NVM Express Controller

Standard NVM Express Controller

Class	Storage controllers
Class GUID	{4d36e97b-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07F0&SUBSYS_07F015AD&REV_00\4&23F707FC&0&00B8
Manufacturer	Standard NVM Express Controller
Location	PCI bus 19, device 0, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SCSIADAPTER
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	stornvme.inf

Storage volumes

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{D7A994E2-ABFF-11EF-8FBE-806E6F6E6963}#0000000ED5C00000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Inf Name	volume.inf

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{D7A994E2-ABFF-11EF-8FBE-806E6F6E6963}#0000000006500000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Inf Name	volume.inf

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{D7A994E2-ABFF-11EF-8FBE-806E6F6E6963}#0000000000100000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Inf Name	volume.inf

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{D7A994E2-ABFF-11EF-8FBE-806E6F6E6963}#0000000007500000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Inf Name	volume.inf

System devices

ACPI Fixed Feature Button

ACPI Fixed Feature Button

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\FIXEDBUTTON\2&DABA3FF&1
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Composite Bus Enumerator

Composite Bus Enumerator

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\COMPOSITEBUS\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	compositebus.inf

CPU to PCI Bridge

CPU to PCI Bridge

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_8086&DEV_7190&SUBSYS_197615AD&REV_01\3&18D45AA6&0&00
Manufacturer	Intel
Location	PCI bus 0, device 0, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Direct memory access controller

Direct memory access controller

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0200\4&25EE97C0&0
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

EISA programmable interrupt controller

EISA programmable interrupt controller

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0001\4&25EE97C0&0
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\44
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\43
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\4&25EE97C0&0
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\41
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\40
Manufacturer	(Standard system devices)

Driver Details	
Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\3F
Manufacturer	(Standard system devices)

Driver Details	
Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\3C
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\3D
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\45
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\3B
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\3A
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\39
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\38
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\3E
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\46
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\4A
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\48
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\57
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\56
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\55
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\54
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\53
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\52
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\47
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\51
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\4F
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\4E
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\4D
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\4C
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\4B
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\49
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\50
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\36
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\37
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\34
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\35
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\1E
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\1D
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\1C
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\1B
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\1A
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\19
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\20
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\18
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\16
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\15
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\14
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\13
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\12
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\11
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\10
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\17
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\21
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\1F
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\23
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\33
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\32
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\31
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\30
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\2F
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\22
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\2D
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\2C
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\2E
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\2A
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\29
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\28
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\27
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\26
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\25
Manufacturer	(Standard system devices)

Driver Details	
Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\24
Manufacturer	(Standard system devices)

Driver Details	
Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\2B
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Generic Bus

Generic Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A05\42
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

High Definition Audio Controller

High Definition Audio Controller

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_1977&SUBSYS_197715AD&REV_09\4&B70F118&0&0888
Manufacturer	Microsoft
Location	PCI bus 2, device 1, function 0

Driver Details

Driver Date	Friday, September 27, 2024 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	hdaudbus.inf

High precision event timer

High precision event timer

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0103\4&25EE97C0&0
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Microsoft ACPI-Compliant System

Microsoft ACPI-Compliant System

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI_HAL\PNP0C08\0
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	acpi.inf

Microsoft Basic Display Driver

Microsoft Basic Display Driver

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\BASICDISPLAY\0000
Manufacturer	(Standard display types)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	basicdisplay.inf

Microsoft Basic Render Driver

Microsoft Basic Render Driver

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\BASICRENDER\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	basicrender.inf

Microsoft Hyper-V Generation Counter

Microsoft Hyper-V Generation Counter

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\VMW0001\7
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	wgencounter.inf

Microsoft System Management BIOS Driver

Microsoft System Management BIOS Driver

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\MSSMBIOS\0000
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Inf Name	mssmbios.inf

Microsoft Virtual Drive Enumerator

Microsoft Virtual Drive Enumerator

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\VDRVROOT\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1591
Inf Name	vdrvroot.inf

Motherboard resources

Motherboard resources	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0C02\4
Manufacturer	(Standard system devices)

Driver Details	
Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

Motherboard resources

Motherboard resources	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0C02\1F
Manufacturer	(Standard system devices)

Driver Details	
Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

NDIS Virtual Network Adapter Enumerator

NDIS Virtual Network Adapter Enumerator	
Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\NDISVIRTUALBUS\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Inf Name	ndisvirtualbus.inf

PCI Bus

PCI Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0A03\2&DABA3FF&1
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&C7
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 24, function 7

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B1
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 22, function 1

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&C5
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 24, function 5

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B7
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 22, function 7

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B6
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 22, function 6

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&C6
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 24, function 6

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B4
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 22, function 4

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B3
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 22, function 3

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B2
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 22, function 2

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B0
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 22, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&AF
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 21, function 7

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&AE
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 21, function 6

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&AD
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 21, function 5

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&AC
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 21, function 4

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&AB
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 21, function 3

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&AA
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 21, function 2

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&A9
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 21, function 1

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&A8
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 21, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B8
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 23, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B9
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 23, function 1

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&B5
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 22, function 5

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&BA
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 23, function 2

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&C0
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 24, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&BE
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 23, function 6

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&BD
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 23, function 5

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&C1
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 24, function 1

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&C2
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 24, function 2

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&BF
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 23, function 7

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&C3
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 24, function 3

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&C4
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 24, function 4

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&BB
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 23, function 3

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07A0&SUBSYS_07A015AD&REV_01\3&18D45AA6&0&BC
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 23, function 4

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI to ISA Bridge

PCI to ISA Bridge

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_8086&DEV_7110&SUBSYS_197615AD&REV_08\3&18D45AA6&0&38
Manufacturer	Intel
Location	PCI bus 0, device 7, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

PCI-to-PCI Bridge

PCI-to-PCI Bridge

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_0790&SUBSYS_079015AD&REV_02\3&18D45AA6&0&88
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 17, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

PCI-to-PCI Bridge

PCI-to-PCI Bridge

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_8086&DEV_7191&SUBSYS_00000000&REV_01\3&18D45AA6&0&08
Manufacturer	(Standard system devices)
Location	PCI bus 0, device 1, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	pci.inf

Plug and Play Software Device Enumerator

Plug and Play Software Device Enumerator

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\SYSTEM\0000
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Sunday, March 31, 2024
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1
Inf Name	swenum.inf

Remote Desktop Device Redirector Bus

Remote Desktop Device Redirector Bus

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\RDPBUS\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	rdpbus.inf

System CMOS/real time clock

System CMOS/real time clock

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0B00\4&25EE97C0&0
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

System speaker

System speaker

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0800\4&25EE97C0&0
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

System timer

System timer

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0100\4&25EE97C0&0
Manufacturer	(Standard system devices)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	machine.inf

UMBus Root Bus Enumerator

UMBus Root Bus Enumerator

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\UMBUS\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	umbus.inf

VMware VMCI Bus Device

VMware VMCI Bus Device

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_0740&SUBSYS_074015AD&REV_10\3&18D45AA6&0&3F
Manufacturer	Broadcom Inc.
Location	PCI bus 0, device 7, function 7

Driver Details

Driver Date	Tuesday, July 9, 2024 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Broadcom Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	9.8.18.1
Inf Name	oem7.inf

VMware VMCI Host Device

VMware VMCI Host Device

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\VMWVMCIHOSTDEV\0000
Manufacturer	Broadcom Inc.

Driver Details

Driver Date	Tuesday, July 9, 2024 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Broadcom Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	9.8.18.1
Inf Name	oem7.inf

Volume Manager

Volume Manager

Class	System devices
Class GUID	{4d36e97d-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ROOT\VOLMGR\0000
Manufacturer	Microsoft

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1150
Inf Name	volmgr.inf

Universal Serial Bus controllers

Standard Enhanced PCI to USB Host Controller

Standard Enhanced PCI to USB Host Controller

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_0770&SUBSYS_077015AD&REV_00\4&B70F118&0&1088
Manufacturer	(Standard USB Host Controller)
Location	PCI bus 2, device 2, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	usbport.inf

Standard Universal PCI to USB Host Controller

Standard Universal PCI to USB Host Controller

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_0774&SUBSYS_197615AD&REV_00\4&B70F118&0&0088
Manufacturer	(Standard USB Host Controller)
Location	PCI bus 2, device 0, function 0

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	usbport.inf

Standard USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)

Standard USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_077A&SUBSYS_077A15AD&REV_00\4&AA0A8D5&0&00B0
Manufacturer	Generic USB xHCI Host Controller
Location	PCI bus 11, device 0, function 0

Driver Details

Driver Date	Thursday, January 23, 2025
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Friendly Name	Standard USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
Inf Name	usbxhci.inf

USB Composite Device

USB Composite Device

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	USB\VID_0E0F&PID_0003\6&21ADF8C6&0&5
Manufacturer	(Standard USB Host Controller)
Location	Port_#0005.Hub_#0003

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	usb.inf

USB Root Hub

USB Root Hub

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	USB\ROOT_HUB\5&17DF1C1B&0
Manufacturer	(Standard USB Host Controller)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	usbport.inf

USB Root Hub

USB Root Hub

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	USB\ROOT_HUB20\5&25F23B66&0
Manufacturer	(Standard USB Host Controller)

Driver Details

Driver Date	Wednesday, June 21, 2006 1:00:00 AM
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.1882
Inf Name	usbport.inf

USB Root Hub (USB 3.0)

USB Root Hub (USB 3.0)

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	USB\ROOT_HUB30\5&9FB4995&0&0
Manufacturer	(Standard USB HUBs)

Driver Details

Driver Date	Thursday, January 23, 2025
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.26100.3037
Inf Name	usbhub3.inf

Physical Memory

This section provides information about the physical memory installed in this machine.

Physical Memory

Total Physical Memory	4,095MB

1 Physical Memory Devices

Identifier	Location	Manufacturer	Capacity
Physical Memory 0	RAM slot #0	VMware Virtual RAM	4,096 MB

Physical Memory 0

This section provides information about the physical memory device installed in this machine.

General Settings

Tag	Physical Memory 0
Capacity	4,096 MB
Device Locator	RAM slot #0
Form Factor	DIMM
Memory Type	Synchronous DRAM
Speed	Unknown

Hardware

Manufacturer	VMware Virtual RAM
Part Number	VMW-4096MB
Serial Number	00000001

Advanced

Data Width	64
Total Width	64
Configured Clock Speed	4,800 MHz
Configured Voltage	0 Millivolts

Printers

Provides details of the printers connected to the Windows machine.

1 Printers

Name	Location	Comment	Share Name
Microsoft Print to PDF			[Not Shared]

Microsoft Print to PDF

Provides details of the printers connected to the Windows machine.

Printer Properties

Comment	
Capabilities	Copies Color
Location	
Port Name	PORTPROMPT:
Print Processor	winprint
Separator Page	

Advanced

Availability	Always available
Priority	1
Spool Mode	Start printing immediately
Enable Advanced Printing Features	True
Hold Mismatched Documents	False
Driver Name	Microsoft Print To PDF

Share Configuration

Share Name	[Not Shared]

Permissions

Type	Principal	Access
Allow	CREATOR OWNER	Manage Documents
Allow	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Manage Documents, Print
Allow	Everyone	Print
Allow	BUILTIN\Administrators	Manage Documents, Manage Printer, Print
Allow	S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-1087000422	Manage Documents, Print

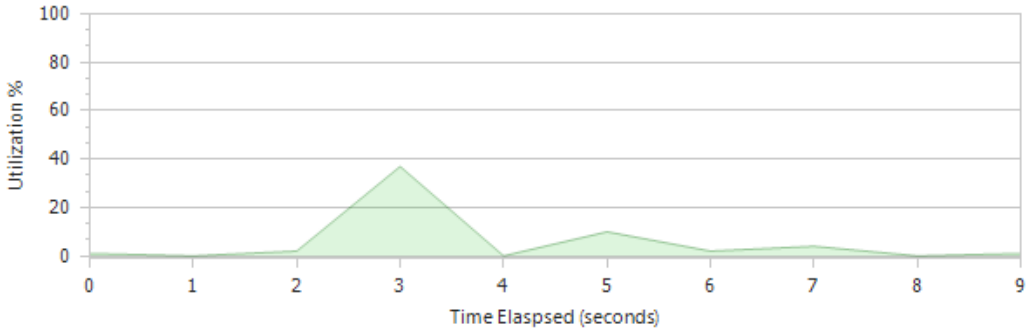
Processors

Displays information about the processors found within this Windows machine as seen by the operating system.

1 Processors

Device ID	Name	Status	Cores
CPU0	Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	Enabled	1

Total Processor Utilization



Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz

Displays information about the processors found within this Windows machine as seen by the operating system.

Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	
CPU Status	Enabled
Current Clock Speed	2,400MHz
Description	Intel64 Family 6 Model 165 Stepping 2
Device Identifier	CPU0
Manufacturer	GenuineIntel
Number Of Cores	1
Number Of Logical Processors	1
Processor Id	0F8BFBFF000A0652
Socket Designation	CPU 0

Cache Information	
Level 2 Cache Size	256KB
Level 3 Cache Size	16,384KB

Virtualization Settings	
Address Translation Extensions	False
Virtualization Firmware Enabled	False

Tape Libraries

Provides information about the tape drives and libraries connected to this machine.

0 Connected Tape Libraries

There are no connected tape libraries.

Trusted Platform Module (TPM)

A trusted platform module (TPM) is a security chip that securely creates and stores cryptographic keys and provides taper protection of the operating system and firmware.

Trusted Platform Module (TPM)	
TPM Present	True
Manufacturer Name	Infineon (IFX)
Manufacturer Identifier	1229346816
Manufacturer Version	7.85.4555.0
Specification Version	2.0
Specification Sub-Version	1.38.0.0

Status	
TPM Activated	True
TPM Ready	True
Locked Out	False

Advanced	
Auto Provisioning Enabled	True
TPM Owned	True
Owner Clear Disabled	False
Owner Password	{Not Documented}
Physical Presence Version	1.3.0.0

Video Controllers

Video controllers, also known as video adapters or graphics cards, are the physical or virtual devices within the machine responsible for generating the display seen by the user.

1 Video Controllers

Name	Adapter Memory	Driver Version
VMware SVGA 3D	256 MB	9.17.7.4

VMware SVGA 3D

DAC Type	n/a
Adapter RAM	256 MB
Driver Date	Tuesday, March 26, 2024
Driver Version	9.17.7.4
Inf Filename	oem6.inf
Drivers	vm3dum64_loader.dll
Maximum Refresh Rate	64Hz
Video Mode Description	3077 x 1991 x 4294967296 colors

Networking

Provides networking information for the Windows machine.

Networking Information	
Network Adapters	5 Network Adapters
IPv4 Addresses	192.168.128.6/22
IPv6 Addresses	fe80::8190:de8d:a907:7f94%7/0.0.0.64

Advanced	
SNMP Installed	False
Routing Table Entries	11
Shares	3

Failover Clustering

A Microsoft failover cluster is a group of independent servers that work together to increase the availability of applications and services.

General Settings	
Enabled	True
Cluster Name	clusterdemo
Fully Qualified Domain Name	clusterdemo.contoso.com

Hosts File

The hosts file is a simple, text based file that is used to map IP addresses to host names.

General

Full Path	C:\WINDOWS\System32\Drivers\etc\hosts
File Size	824 bytes
Creation Date	Monday, April 1, 2024 8:01:27 AM
Last Accessed	Monday, April 1, 2024 8:01:27 AM
Last Modified	Monday, April 1, 2024 8:01:27 AM
File Type	
Hidden	False
Read Only	False

Advanced

Encrypted	False
Compressed	False

Security

Owner	NT AUTHORITY\SYSTEM

5 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
ALL APPLICATION PACKAGES	True	Allow	Read & execute	This folder or file only
ALL RESTRICTED APPLICATION PACKAGES	True	Allow	Read & execute	This folder or file only
BUILTIN\Administrators	True	Allow	Full control	This folder or file only
BUILTIN\Users	True	Allow	Read & execute	This folder or file only
NT AUTHORITY\SYSTEM	True	Allow	Full control	This folder or file only

0 NTFS Audit Rules

There are no audit rules found.

File Contents

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
```

```
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
```

IPv4 Routing Table

The routing table lists the routes to particular network destinations and the metrics (distances or costs) associated with those routes.

11 Active Routes

Destination	Subnet Mask	Gateway	Interface	Metric	Protocol
255.255.255.255	255.255.255.255	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
255.255.255.255	255.255.255.255	0.0.0.0		331	Local
224.0.0.0	240.0.0.0	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
224.0.0.0	240.0.0.0	0.0.0.0		331	Local
192.168.131.255	255.255.255.255	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
192.168.128.6	255.255.255.255	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
192.168.128.0	255.255.252.0	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
127.255.255.255	255.255.255.255	0.0.0.0		331	Local
127.0.0.1	255.255.255.255	0.0.0.0		331	Local
127.0.0.0	255.0.0.0	0.0.0.0		331	Local
0.0.0.0	0.0.0.0	192.168.131.2	Intel(R) 82574L Gigabit Network Connection	25	NetMgmt

Network Adapters

A network adapter, also known as network interface, is a physical or virtual device used to connect a device to the network. The network adapters included within this documentation may include both wired and wireless adapters.

5 Network Adapters

Name	Status	Device Name	MAC address
6to4 Adapter	Device is working properly.		
Ethernet (Kernel Debugger)	Device is working properly.	Microsoft Kernel Debug Network Adapter	
Ethernet0	Device is working properly.	Intel(R) 82574L Gigabit Network Connection	00-0C-29-DA-F1-74
Microsoft IP-HTTPS Platform Interface	Device is working properly.		
Teredo Tunneling Pseudo-Interface	Device is working properly.		

6to4 Adapter

A network adapter, also known as network interface, is a physical or virtual device used to connect a device to the network.

6to4 Adapter	
Index	0002
Device Name	
MAC Address	
Status	Device is working properly.
Driver Date	
Driver Version	
Physical Adapter	False
Interface GUID	{07374750-E68B-490E-9330-9FD785CD71B6}
Speed / Duplex	0 bps

Ethernet (Kernel Debugger)

A network adapter, also known as network interface, is a physical or virtual device used to connect a device to the network.

Ethernet (Kernel Debugger)	
Index	0008
Device Name	Microsoft Kernel Debug Network Adapter
MAC Address	
Status	Device is working properly.
Driver Date	2006-06-21
Driver Version	10.0.26100.1150
Physical Adapter	False
Interface GUID	{502F750F-3800-438B-8EB7-45843E2AF674}
Speed / Duplex	0 bps

Ethernet0

A network adapter, also known as network interface, is a physical or virtual device used to connect a device to the network.

Ethernet0

Index	0007
Device Name	Intel(R) 82574L Gigabit Network Connection
MAC Address	00-0C-29-DA-F1-74
Status	Device is working properly.
Driver Date	2015-08-03
Driver Version	12.19.1.32
Physical Adapter	True
Interface GUID	{40F7F604-29C6-41BF-8EE8-BA34CD7257A5}
Speed / Duplex	1 Gbps [Full Duplex]

Network Adapter Bindings

Name	Class Name	Enabled
Client for Microsoft Networks	Client	True
File and Printer Sharing for Microsoft Networks	Service	True
Internet Protocol Version 4 (TCP/IPv4)	Transport	True
Internet Protocol Version 6 (TCP/IPv6)	Transport	True
Link-Layer Topology Discovery Mapper I/O Driver	Transport	True
Link-Layer Topology Discovery Responder	Transport	True
Microsoft LLDP Protocol Driver	Transport	True
Microsoft Network Adapter Multiplexor Protocol	Transport	False
QoS Packet Scheduler	Filter	True

Network Category

Name	Domain network

IP Configuration

DHCP Enabled	True
IP Addresses	fe80::8190:de8d:a907:7f94%7/0.0.0.64 192.168.128.6/22
Default Gateways	192.168.131.2
DHCP Server	192.168.128.255

DNS Settings

DNS Hostname	XCS-2K25-DEMO
DNS Domain	localdomain
DNS Suffixes	contoso.com localdomain
DNS Servers	192.168.131.112
Register in DNS	True
Use Connection's Suffix in DNS Registration	False

WINS Settings

Primary WINS Server	192.168.131.2
Secondary WINS Server	
Enable LMHOSTS Lookup	True
NetBIOS Setting	Enabled via DHCP

Advanced Properties

Display Name	Name	Display Value	Data
Adaptive Inter-Frame Spacing	AdaptiveIFS	Disabled	0
Flow Control	*FlowControl	Rx & Tx Enabled	3
Gigabit Master Slave Mode	MasterSlave	Auto Detect	0
Interrupt Moderation	*InterruptModeration	Enabled	1
Interrupt Moderation Rate	ITR	Adaptive	65535
IPv4 Checksum Offload	*IPChecksumOffloadIPv4	Rx & Tx Enabled	3
Jumbo Packet	*JumboPacket	Disabled	1514
Large Send Offload V2 (IPv4)	*LsoV2IPv4	Enabled	1
Large Send Offload V2 (IPv6)	*LsoV2IPv6	Enabled	1
Locally Administered Address	NetworkAddress		
Log Link State Event	LogLinkStateEvent	Enabled	51
Maximum number of RSS Processors	*MaxRssProcessors	8	8
Maximum Number of RSS Queues	*NumRssQueues	2 Queues	2
Maximum RSS Processor Number	*RssMaxProcNumber	63	63
Packet Priority & VLAN	*PriorityVLANTag	Packet Priority & VLAN Enabled	3
Preferred NUMA node	*NumaNodeId	65535	65535
Receive Buffers	*ReceiveBuffers	256	256
Receive Side Scaling	*RSS	Enabled	1
RSS Base Processor Number	*RssBaseProcNumber	0	0
RSS load balancing profile	*RSSProfile	NUMAScalingStatic	4
Speed & Duplex	*SpeedDuplex	Auto Negotiation	0
TCP Checksum Offload (IPv4)	*TCPChecksumOffloadIPv4	Rx & Tx Enabled	3
TCP Checksum Offload (IPv6)	*TCPChecksumOffloadIPv6	Rx & Tx Enabled	3

Transmit Buffers	*TransmitBuffers	512	512
UDP Checksum Offload (IPv4)	*UDPChecksumOffloadIPv4	Rx & Tx Enabled	3
UDP Checksum Offload (IPv6)	*UDPChecksumOffloadIPv6	Rx & Tx Enabled	3
Wait for Link	WaitAutoNegComplete	Auto Detect	2

Microsoft IP-HTTPS Platform Interface

A network adapter, also known as network interface, is a physical or virtual device used to connect a device to the network.

Microsoft IP-HTTPS Platform Interface	
Index	0006
Device Name	
MAC Address	
Status	Device is working properly.
Driver Date	
Driver Version	
Physical Adapter	False
Interface GUID	{2EE2C70C-A092-4D88-A654-98C8D7645CD5}
Speed / Duplex	0 bps

Teredo Tunneling Pseudo-Interface

A network adapter, also known as network interface, is a physical or virtual device used to connect a device to the network.

Teredo Tunneling Pseudo-Interface	
Index	0010
Device Name	
MAC Address	
Status	Device is working properly.
Driver Date	
Driver Version	
Physical Adapter	False
Interface GUID	{93123211-9629-4E04-82F0-EA2E4F221468}
Speed / Duplex	0 bps

Network Load Balancing

Microsoft network load balancing (NLB) increases the availability and scalability of Internet server applications such as web, FTP, firewall, and proxy.

General Settings	
Enabled	False

Remote Assistance

Windows Remote Assistance allows a trusted expert to remotely take over a Windows machine.

Remote Assistance Settings	
Enabled	False

Remote Desktop

Remote Desktop allows users running an appropriate version of the Remote Desktop client to connect to a remote machine and access the desktop or published applications using the Remote Desktop Protocol (RDP).

Remote Desktop Settings	
Connection Mode	Don't allow remote connections
Licensing Type	Remote Desktop for Administration

SNMP Configuration

Simple Network Management Protocol (SNMP) is a UDP-based network protocol used by network monitoring and management systems. SNMP is protected by the use of passwords known as community strings and by allowing connections from specific hosts only. SNMP traps define the management hosts that will receive event messages from this machine.

SNMP Settings

Installed	False

Shares

Windows shares allow the sharing of files and printers over a network using the Server Message Block (SMB) protocol, also known as Common Internet File System (CIFS).

3 Shares

Name	Path	Type	Description
ADMIN$	C:\WINDOWS	Administrative Share	Remote Admin
C$	C:\	Administrative Share	Default share
IPC$		Administrative IPC Queue	Remote IPC

ADMIN$

ADMIN$

Description	Remote Admin
Allow Maximum	True
Path	C:\WINDOWS
Share Type	Administrative Share
Cache Setting	Only files and folders that users specify are available offline.

Security

Owner	NT SERVICE\TrustedInstaller

9 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
ALL APPLICATION PACKAGES	False	Allow	Read & execute	This folder, subfolders and files
ALL RESTRICTED APPLICATION PACKAGES	False	Allow	Read & execute	This folder, subfolders and files
BUILTIN\Administrators	False	Allow	Full control	Subfolders and files only
BUILTIN\Administrators	False	Allow	Modify	This folder or file only
BUILTIN\Users	False	Allow	Read & execute	This folder, subfolders and files
CREATOR OWNER	False	Allow	Full control	Subfolders and files only
NT AUTHORITY\SYSTEM	False	Allow	Full control	Subfolders and files only
NT AUTHORITY\SYSTEM	False	Allow	Modify	This folder or file only
NT SERVICE\TrustedInstaller	False	Allow	Full control	This folder and subfolders

0 NTFS Audit Rules

There are no audit rules found.

C$

C$

Description	Default share
Allow Maximum	True
Path	C:\
Share Type	Administrative Share
Cache Setting	Only files and folders that users specify are available offline.

Security

Owner	NT SERVICE\TrustedInstaller

7 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
BUILTIN\Administrators	False	Allow	Full control	This folder, subfolders and files
BUILTIN\Users	False	Allow	Read & execute	This folder, subfolders and files
BUILTIN\Users	False	Allow	Create folders / append data	This folder and subfolders
BUILTIN\Users	False	Allow	Create files / write data	Subfolders only
CREATOR OWNER	False	Allow	Full control	Subfolders and files only
NT AUTHORITY\SYSTEM	False	Allow	Full control	This folder, subfolders and files
S-1-15-3-65536-1888954469-739942743-1668119174-2468466756-4239452838-1296943325-355587736-700089176	False	Allow	List folder / read data Read attributes Traverse folder / execute file	This folder or file only

0 NTFS Audit Rules

There are no audit rules found.

IPC$

IPC$

Description	Remote IPC
Allow Maximum	True
Path	
Share Type	Administrative IPC Queue

Security

Provides details of the key built-in security accounts on this machine.

Security Identifiers

Machine SID	S-1-5-21-346512116-3600583813-593958679
Computer Domain SID	S-1-5-21-3658165781-1802088474-919021730-1116

Local Administrator

Name	Administrator
Description	Built-in account for administering the computer/domain
Enabled	True
Password Never Expires	True

Guest Account

Name	Guest
Description	Built-in account for guest access to the computer/domain
Enabled	False
Password Never Expires	True

Local Administrators

Name	Administrators
Description	Administrators have complete and unrestricted access to the computer/domain
Members	CONTOSO\Domain Admins XCS-2K25-DEMO\Administrator

Advanced Audit Policy

Advanced Audit Policy in Windows 7, Windows Server 2008 R2 and above increase the nine basic audit categories available in previous versions of Windows helping with audit compliance and security monitoring.

Advanced Audit Policy		
Subcategory	**Audit Events**	**Configuration Source**
Account Logon		
Audit Credential Validation	Success	Local
Audit Kerberos Authentication Service	Success	Local
Audit Kerberos Service Ticket Operations	Success	Local
Audit Other Account Logon Events	None	Local
Account Management		
Audit Application Group Management	None	Local
Audit Computer Account Management	Success	Local
Audit Distribution Group Management	None	Local
Audit Other Account Management Events	None	Local
Audit Security Group Management	Success	Local
Audit User Account Management	Success	Local
Detailed Tracking		
Audit DPAPI Activity	None	Local
Audit PNP Activity	None	Local
Audit Process Creation	None	Local
Audit Process Termination	None	Local
Audit RPC Events	None	Local
DS Access		
Audit Detailed Directory Service Replication	None	Local
Audit Directory Service Access	Success	Local
Audit Directory Service Changes	None	Local
Audit Directory Service Replication	None	Local
Logon/Logoff		
Audit Account Lockout	Success	Local
Audit Group Membership	None	Local
Audit IPsec Extended Mode	None	Local
Audit IPsec Main Mode	None	Local
Audit IPsec Quick Mode	None	Local
Audit Logoff	Success	Local
Audit Logon	Success and Failure	Local

Audit Network Policy Server	Success and Failure	Local
Audit Other Logon/Logoff Events	None	Local
Audit Special Logon	Success	Local
Audit User / Device Claims	None	Local
Object Access		
Audit Application Generated	None	Local
Audit Central Access Policy Staging	None	Local
Audit Certification Services	None	Local
Audit Detailed File Share	None	Local
Audit File Share	None	Local
Audit File System	None	Local
Audit Filtering Platform Connection	None	Local
Audit Filtering Platform Packet Drop	None	Local
Audit Handle Manipulation	None	Local
Audit Kernel Object	None	Local
Audit Other Object Access Events	None	Local
Audit Registry	None	Local
Audit Removable Storage	None	Local
Audit SAM	None	Local
Policy Change		
Audit Audit Policy Change	Success	Local
Audit Authentication Policy Change	Success	Local
Audit Authorization Policy Change	None	Local
Audit Filtering Platform Policy Change	None	Local
Audit MPSSVC Rule-Level Policy Change	None	Local
Audit Other Policy Change Events	None	Local
Privilege Use		
Audit Non Sensitive Privilege Use	None	Local
Audit Other Privilege Use Events	None	Local
Audit Sensitive Privilege Use	None	Local
System		
Audit IPsec Driver	None	Local
Audit Other System Events	Success and Failure	Local
Audit Security State Change	Success	Local
Audit Security System Extension	None	Local
Audit System Integrity	Success and Failure	Local

Audit Policy

The audit policy determines what categories of information should be recorded to the Windows Security event log.

Name	Policy Setting	Configuration Source
Audit account logon events	None	Configured Locally
Audit account management	None	Configured Locally
Audit directory service access	None	Configured Locally
Audit logon events	None	Configured Locally
Audit object access	None	Configured Locally
Audit policy change	None	Configured Locally
Audit privilege use	None	Configured Locally
Audit process tracking	None	Configured Locally
Audit system events	None	Configured Locally

Certificate Stores

Provides details of the SSL certificates installed on this machine for the computer account.

Store Name	Certificate Count
Intermediate Certification Authorities	3
Personal	1
Third-Party Root Certification Authorities	7
Trusted People	0
Trusted Publisher	0
Trusted Root Certification Authorities	13
Web Hosting	0

Intermediate Certification Authorities

Intermediate Certification Authorities allows a root certification authority to delegate the ability to create certificates to subordinates.

An Intermediate Certification Authority has the ability to issue server certificates, personal certificates, publisher certificates, or certificates for other Intermediate Certification Authorities.

3 Certificates

Issued To	Issuer	Expiry Date
Microsoft Windows Hardware Compatibility	Microsoft Root Authority	Tuesday, December 31, 2002
Root Agency	Root Agency	Saturday, December 31, 2039
www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign	Class 3 Public Primary Certification Authority	Monday, October 24, 2016

Microsoft Windows Hardware Compatibility

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft Windows Hardware Compatibility
Subject	CN=Microsoft Windows Hardware Compatibility, OU=Microsoft Corporation, OU=Microsoft Windows Hardware Compatibility Intermediate CA, OU=Copyright (c) 1997 Microsoft Corp.
Has Private Key	False
Issuer	CN=Microsoft Root Authority, OU=Microsoft Corporation, OU=Copyright (c) 1997 Microsoft Corp.
Issuer Name	Microsoft Root Authority
Valid From	Wednesday, October 1, 1997
Expiry Date	Tuesday, December 31, 2002
Key Usage	
Enhanced Key Usages	Code Signing (1.3.6.1.5.5.7.3.3) Windows Hardware Driver Verification (1.3.6.1.4.1.311.10.3.5)

Certificate Details

Public Key	RSA (1024 Bits)
Serial Number	198B11D13F9A8FFE69A0
Signature Algorithm	md5RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	
Thumbprint	109F1CAED645BB78B3EA2B94C0697C740733031C
Purposes	Enable all purposes for this certificate

Root Agency

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Root Agency
Subject	CN=Root Agency
Has Private Key	False
Issuer	CN=Root Agency
Issuer Name	Root Agency
Valid From	Tuesday, May 28, 1996
Expiry Date	Saturday, December 31, 2039
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (512 Bits)
Serial Number	06376C00AA00648A11CFB8D4AA5C35F4
Signature Algorithm	md5RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	
Thumbprint	FEE449EE0E3965A5246F000E87FDE2A065FD89D4
Purposes	Enable all purposes for this certificate

www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
Subject	OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign, OU=VeriSign International Server CA - Class 3, OU="VeriSign, Inc.", O=VeriSign Trust Network
Has Private Key	False
Issuer	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Issuer Name	Class 3 Public Primary Certification Authority
Valid From	Thursday, April 17, 1997
Expiry Date	Monday, October 24, 2016
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Unknown Key Usage (2.16.840.1.113730.4.1) Unknown Key Usage (2.16.840.1.113733.1.8.1)

Certificate Details

Public Key	RSA (1024 Bits)
Serial Number	46FCEBBAB4D02F0F926098233F93078F
Signature Algorithm	sha1RSA
Version	3
CRL Distribution Points	http://crl.verisign.com/pca3.crl
Subject Alternative Names	

Properties

Friendly Name	
Thumbprint	D559A586669B08F46A30A133F8A9ED3D038E2EA8
Purposes	Enable all purposes for this certificate

Personal

Certificates associated with private keys to which you have access. These are the certificates that have been issued to you or to the computer or service for which you are managing certificates.

1 Certificates

Issued To	Issuer	Expiry Date
WMSvc-SHA2-XCS-2K25-DEMO	WMSvc-SHA2-XCS-2K25-DEMO	Monday, January 1, 2035

WMSvc-SHA2-XCS-2K25-DEMO

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	WMSvc-SHA2-XCS-2K25-DEMO
Subject	CN=WMSvc-SHA2-XCS-2K25-DEMO
Has Private Key	True
Issuer	CN=WMSvc-SHA2-XCS-2K25-DEMO
Issuer Name	WMSvc-SHA2-XCS-2K25-DEMO
Valid From	Friday, January 3, 2025
Expiry Date	Monday, January 1, 2035
Key Usage	Data encipherment Digital Signature Key encipherment
Enhanced Key Usages	Server Authentication (1.3.6.1.5.5.7.3.1)

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	189F234BCCB3EE984F8A637ACECFCE6A
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	WMSVC-SHA2
Thumbprint	99AFA923918E35A362EADB0D37C31F2AAD802EA4
Purposes	Enable all purposes for this certificate

Third-Party Root Certification Authorities

Third-Party Root Certification Authorities contains certificates from CAs other than Microsoft and your organisation.

7 Certificates

Issued To	Issuer	Expiry Date
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certification Authority	Tuesday, August 1, 2028
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	Monday, November 10, 2031
DigiCert Global Root CA	DigiCert Global Root CA	Monday, November 10, 2031
DigiCert Global Root G2	DigiCert Global Root G2	Friday, January 15, 2038
DigiCert Global Root G3	DigiCert Global Root G3	Friday, January 15, 2038
GlobalSign Root CA	GlobalSign Root CA	Friday, January 28, 2028
Microsoft RSA Root Certificate Authority 2017	Microsoft RSA Root Certificate Authority 2017	Friday, July 18, 2042

Class 3 Public Primary Certification Authority

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Class 3 Public Primary Certification Authority
Subject	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Has Private Key	False
Issuer	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Issuer Name	Class 3 Public Primary Certification Authority
Valid From	Monday, January 29, 1996
Expiry Date	Tuesday, August 1, 2028
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (1024 Bits)
Serial Number	70BAE41D10D92934B638CA7B03CCBABF
Signature Algorithm	md2RSA
Version	1
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	VeriSign Class 3 Public Primary CA
Thumbprint	742C3192E607E424EB4549542BE1BBC53E6174E2
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1)

DigiCert Assured ID Root CA

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	DigiCert Assured ID Root CA
Subject	CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Has Private Key	False
Issuer	CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer Name	DigiCert Assured ID Root CA
Valid From	Friday, November 10, 2006
Expiry Date	Monday, November 10, 2031
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	0CE7E0E517D846FE8FE560FC1BF03039
Signature Algorithm	sha1RSA
Authority Key Identifier	45eba2aff492cb82312d518ba7a7219df36dc80f
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	DigiCert
Thumbprint	0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

DigiCert Global Root CA

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	DigiCert Global Root CA
Subject	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Has Private Key	False
Issuer	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer Name	DigiCert Global Root CA
Valid From	Friday, November 10, 2006
Expiry Date	Monday, November 10, 2031
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	083BE056904246B1A1756AC95991C74A
Signature Algorithm	sha1RSA
Authority Key Identifier	03de503556d14cbb66f0a3e21b1bc397b23dd155
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	DigiCert
Thumbprint	A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

DigiCert Global Root G2

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	DigiCert Global Root G2
Subject	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
Has Private Key	False
Issuer	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer Name	DigiCert Global Root G2
Valid From	Thursday, August 1, 2013
Expiry Date	Friday, January 15, 2038
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	033AF1E6A711A9A0BB2864B11D09FAE5
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	DigiCert Global Root G2
Thumbprint	DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

DigiCert Global Root G3

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	DigiCert Global Root G3
Subject	CN=DigiCert Global Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
Has Private Key	False
Issuer	CN=DigiCert Global Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer Name	DigiCert Global Root G3
Valid From	Thursday, August 1, 2013
Expiry Date	Friday, January 15, 2038
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	ECC (384 Bits)
Serial Number	055556BCF25EA43535C3A40FD5AB4572
Signature Algorithm	sha384ECDSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	DigiCert Global Root G3
Thumbprint	7E04DE896A3E666D00E687D33FFAD93BE83D349E
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

GlobalSign Root CA

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	GlobalSign Root CA
Subject	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Has Private Key	False
Issuer	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Issuer Name	GlobalSign Root CA
Valid From	Tuesday, September 1, 1998
Expiry Date	Friday, January 28, 2028
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	040000000001154B5AC394
Signature Algorithm	sha1RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	GlobalSign Root CA - R1
Thumbprint	B1BC968BD4F49D622AA89A81F2150152A41D829C
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Encrypting File System (1.3.6.1.4.1.311.10.3.4) Secure Email (1.3.6.1.5.5.7.3.4) IP security IKE intermediate (1.3.6.1.5.5.8.2.2) IP security tunnel termination (1.3.6.1.5.5.7.3.6) IP security user (1.3.6.1.5.5.7.3.7) OCSP Signing (1.3.6.1.5.5.7.3.9) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

Microsoft RSA Root Certificate Authority 2017

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft RSA Root Certificate Authority 2017
Subject	CN=Microsoft RSA Root Certificate Authority 2017, O=Microsoft Corporation, C=US
Has Private Key	False
Issuer	CN=Microsoft RSA Root Certificate Authority 2017, O=Microsoft Corporation, C=US
Issuer Name	Microsoft RSA Root Certificate Authority 2017
Valid From	Wednesday, December 18, 2019
Expiry Date	Friday, July 18, 2042
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (4096 Bits)
Serial Number	1ED397095FD8B4B347701EAABE7F45B3
Signature Algorithm	sha384RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft RSA Root Certificate Authority 2017
Thumbprint	73A5E64A3BFF8316FF0EDCCC618A906E4EAE4D74
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1)

Trusted People

Certificates issued to people or end entities that are explicitly trusted. Certificates in the Trusted People store are considered trusted by default and are not verified by higher authorities or certificate trust lists or chains.

There are no certificates in this store.

Trusted Publisher

The Trusted Publishers certificate store contains information about the Authenticode (signing) certificates of trusted publishers that are installed on a computer.

There are no certificates in this store.

Trusted Root Certification Authorities

Trusted Root Certification Authorities contains root certificates from your organisation and Microsoft. Please note, unlike the Microsoft Certificates MMC this does NOTE also include the certificates from the Third-Party Root Certification Authorities.

13 Certificates

Issued To	Issuer	Expiry Date
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	Thursday, December 30, 1999
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	Friday, December 31, 1999
Microsoft ECC Product Root Certificate Authority 2018	Microsoft ECC Product Root Certificate Authority 2018	Friday, February 27, 2043
Microsoft ECC TS Root Certificate Authority 2018	Microsoft ECC TS Root Certificate Authority 2018	Friday, February 27, 2043
Microsoft Root Authority	Microsoft Root Authority	Thursday, December 31, 2020
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	Sunday, May 9, 2021
Microsoft Root Certificate Authority 2010	Microsoft Root Certificate Authority 2010	Saturday, June 23, 2035
Microsoft Root Certificate Authority 2011	Microsoft Root Certificate Authority 2011	Saturday, March 22, 2036
Microsoft Time Stamp Root Certificate Authority 2014	Microsoft Time Stamp Root Certificate Authority 2014	Saturday, October 22, 2039
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	Wednesday, January 7, 2004
Symantec Enterprise Mobile Root for Microsoft	Symantec Enterprise Mobile Root for Microsoft	Sunday, March 14, 2032
Thawte Timestamping CA	Thawte Timestamping CA	Thursday, December 31, 2020
WMSvc-SHA2-XCS-2K25-DEMO	WMSvc-SHA2-XCS-2K25-DEMO	Monday, January 1, 2035

Copyright (c) 1997 Microsoft Corp.

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Copyright (c) 1997 Microsoft Corp.
Subject	OU=Copyright (c) 1997 Microsoft Corp., OU=Microsoft Time Stamping Service Root, OU=Microsoft Corporation, O=Microsoft Trust Network
Has Private Key	False
Issuer	OU=Copyright (c) 1997 Microsoft Corp., OU=Microsoft Time Stamping Service Root, OU=Microsoft Corporation, O=Microsoft Trust Network
Issuer Name	Copyright (c) 1997 Microsoft Corp.
Valid From	Tuesday, May 13, 1997
Expiry Date	Thursday, December 30, 1999
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (1024 Bits)
Serial Number	01
Signature Algorithm	md5RSA
Version	1
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft Timestamp Root
Thumbprint	245C97DF7514E7CF2DF8BE72AE957B9E04741E85
Purposes	Time Stamping (1.3.6.1.5.5.7.3.8)

Microsoft Authenticode(tm) Root Authority

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft Authenticode(tm) Root Authority
Subject	CN=Microsoft Authenticode(tm) Root Authority, O=MSFT, C=US
Has Private Key	False
Issuer	CN=Microsoft Authenticode(tm) Root Authority, O=MSFT, C=US
Issuer Name	Microsoft Authenticode(tm) Root Authority
Valid From	Sunday, January 1, 1995
Expiry Date	Friday, December 31, 1999
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	01
Signature Algorithm	md5RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft Authenticode(tm) Root
Thumbprint	7F88CD7223F3C813818C994614A89C99FA3B5247
Purposes	Secure Email (1.3.6.1.5.5.7.3.4) Code Signing (1.3.6.1.5.5.7.3.3)

Microsoft ECC Product Root Certificate Authority 2018

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft ECC Product Root Certificate Authority 2018
Subject	CN=Microsoft ECC Product Root Certificate Authority 2018, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Has Private Key	False
Issuer	CN=Microsoft ECC Product Root Certificate Authority 2018, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Issuer Name	Microsoft ECC Product Root Certificate Authority 2018
Valid From	Tuesday, February 27, 2018
Expiry Date	Friday, February 27, 2043
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	ECC (384 Bits)
Serial Number	14982666DC7CCD8F4053677BB999EC85
Signature Algorithm	sha384ECDSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft ECC Product Root Certificate Authority 2018
Thumbprint	06F1AA330B927B753A40E68CDF22E34BCBEF3352
Purposes	Enable all purposes for this certificate

Microsoft ECC TS Root Certificate Authority 2018

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft ECC TS Root Certificate Authority 2018
Subject	CN=Microsoft ECC TS Root Certificate Authority 2018, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Has Private Key	False
Issuer	CN=Microsoft ECC TS Root Certificate Authority 2018, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Issuer Name	Microsoft ECC TS Root Certificate Authority 2018
Valid From	Tuesday, February 27, 2018
Expiry Date	Friday, February 27, 2043
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	ECC (384 Bits)
Serial Number	153875E1647ED1B047B4EFAF41128245
Signature Algorithm	sha384ECDSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft ECC TS Root Certificate Authority 2018
Thumbprint	31F9FC8BA3805986B721EA7295C65B3A44534274
Purposes	Enable all purposes for this certificate

Microsoft Root Authority

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft Root Authority
Subject	CN=Microsoft Root Authority, OU=Microsoft Corporation, OU=Copyright (c) 1997 Microsoft Corp.
Has Private Key	False
Issuer	CN=Microsoft Root Authority, OU=Microsoft Corporation, OU=Copyright (c) 1997 Microsoft Corp.
Issuer Name	Microsoft Root Authority
Valid From	Friday, January 10, 1997
Expiry Date	Thursday, December 31, 2020
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	00C1008B3C3C8811D13EF663ECDF40
Signature Algorithm	md5RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft Root Authority
Thumbprint	A43489159A520F0D93D032CCAF37E7FE20A8B419
Purposes	Enable all purposes for this certificate

Microsoft Root Certificate Authority

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft Root Certificate Authority
Subject	CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com
Has Private Key	False
Issuer	CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com
Issuer Name	Microsoft Root Certificate Authority
Valid From	Wednesday, May 9, 2001
Expiry Date	Sunday, May 9, 2021
Key Usage	Certificate signing CRL signing Digital Signature Non-repudiation
Enhanced Key Usages	

Certificate Details

Public Key	RSA (4096 Bits)
Serial Number	79AD16A14AA0A5AD4C7358F407132E65
Signature Algorithm	sha1RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft Root Certificate Authority
Thumbprint	CDD4EEAE6000AC7F40C3802C171E30148030C072
Purposes	Enable all purposes for this certificate

Microsoft Root Certificate Authority 2010

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft Root Certificate Authority 2010
Subject	CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Has Private Key	False
Issuer	CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Issuer Name	Microsoft Root Certificate Authority 2010
Valid From	Wednesday, June 23, 2010
Expiry Date	Saturday, June 23, 2035
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (4096 Bits)
Serial Number	28CC3A25BFBA44AC449A9B586B4339AA
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft Root Certificate Authority 2010
Thumbprint	3B1EFD3A66EA28B16697394703A72CA340A05BD5
Purposes	Enable all purposes for this certificate

Microsoft Root Certificate Authority 2011

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft Root Certificate Authority 2011
Subject	CN=Microsoft Root Certificate Authority 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Has Private Key	False
Issuer	CN=Microsoft Root Certificate Authority 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Issuer Name	Microsoft Root Certificate Authority 2011
Valid From	Tuesday, March 22, 2011
Expiry Date	Saturday, March 22, 2036
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (4096 Bits)
Serial Number	3F8BC8B5FC9FB29643B569D66C42E144
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft Root Certificate Authority 2011
Thumbprint	8F43288AD272F3103B6FB1428485EA3014C0BCFE
Purposes	Enable all purposes for this certificate

Microsoft Time Stamp Root Certificate Authority 2014

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Microsoft Time Stamp Root Certificate Authority 2014
Subject	CN=Microsoft Time Stamp Root Certificate Authority 2014, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Has Private Key	False
Issuer	CN=Microsoft Time Stamp Root Certificate Authority 2014, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Issuer Name	Microsoft Time Stamp Root Certificate Authority 2014
Valid From	Wednesday, October 22, 2014
Expiry Date	Saturday, October 22, 2039
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (4096 Bits)
Serial Number	2FD67A432293329045E953343EE27466
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Microsoft Time Stamp Root Certificate Authority 2014
Thumbprint	0119E81BE9A14CD8E22F40AC118C687ECBA3F4D8
Purposes	Enable all purposes for this certificate

NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
Subject	OU="NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.", OU=VeriSign Time Stamping Service Root, OU="VeriSign, Inc.", O=VeriSign Trust Network
Has Private Key	False
Issuer	OU="NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.", OU=VeriSign Time Stamping Service Root, OU="VeriSign, Inc.", O=VeriSign Trust Network
Issuer Name	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
Valid From	Monday, May 12, 1997
Expiry Date	Wednesday, January 7, 2004
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (1024 Bits)
Serial Number	4A19D2388C82591CA55D735F155DDCA3
Signature Algorithm	md5RSA
Version	1
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	VeriSign Time Stamping CA
Thumbprint	18F7C1FCC3090203FD5BAA2F861A754976C8DD25
Purposes	Time Stamping (1.3.6.1.5.5.7.3.8)

Symantec Enterprise Mobile Root for Microsoft

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Symantec Enterprise Mobile Root for Microsoft
Subject	CN=Symantec Enterprise Mobile Root for Microsoft, O=Symantec Corporation, C=US
Has Private Key	False
Issuer	CN=Symantec Enterprise Mobile Root for Microsoft, O=Symantec Corporation, C=US
Issuer Name	Symantec Enterprise Mobile Root for Microsoft
Valid From	Thursday, March 15, 2012
Expiry Date	Sunday, March 14, 2032
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	0F6B552F9EBF907B0F6629A9BDF4D8CE
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	DirectoryAddress:CN=MPKI-2048-1-111

Properties

Friendly Name	
Thumbprint	92B46C76E13054E104F230517E6E504D43AB10B5
Purposes	Code Signing (1.3.6.1.5.5.7.3.3)

Thawte Timestamping CA

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	Thawte Timestamping CA
Subject	CN=Thawte Timestamping CA, OU=Thawte Certification, O=Thawte, L=Durbanville, S=Western Cape, C=ZA
Has Private Key	False
Issuer	CN=Thawte Timestamping CA, OU=Thawte Certification, O=Thawte, L=Durbanville, S=Western Cape, C=ZA
Issuer Name	Thawte Timestamping CA
Valid From	Wednesday, January 1, 1997
Expiry Date	Thursday, December 31, 2020
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (1024 Bits)
Serial Number	00
Signature Algorithm	md5RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Thawte Timestamping CA
Thumbprint	BE36A4562FB2EE05DBB3D32323ADF445084ED656
Purposes	Time Stamping (1.3.6.1.5.5.7.3.8)

WMSvc-SHA2-XCS-2K25-DEMO

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	WMSvc-SHA2-XCS-2K25-DEMO
Subject	CN=WMSvc-SHA2-XCS-2K25-DEMO
Has Private Key	True
Issuer	CN=WMSvc-SHA2-XCS-2K25-DEMO
Issuer Name	WMSvc-SHA2-XCS-2K25-DEMO
Valid From	Friday, January 3, 2025
Expiry Date	Monday, January 1, 2035
Key Usage	Data encipherment Digital Signature Key encipherment
Enhanced Key Usages	Server Authentication (1.3.6.1.5.5.7.3.1)

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	189F234BCCB3EE984F8A637ACECFCE6A
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	WMSVC-SHA2
Thumbprint	99AFA923918E35A362EADB0D37C31F2AAD802EA4
Purposes	Enable all purposes for this certificate

Web Hosting

The Web Hosting certificate store contains information about the web hosting certificates that are installed on a computer. This is a new store available in Windows 8, Windows Server 2012 and above.

There are no certificates in this store.

Local Account Policies

Local account policies define the password complexity and account lockout policies that are effective on an individual machine. These policies can be configured locally or via a Group Policy Object (GPO).

Account Lockout Policy

Policy	Policy Setting	Configuration Source
Account lockout duration	Not Applicable	Configured Locally
Account lockout threshold	0 invalid login attempt(s)	Default Domain Policy
Reset account lockout counter after	Not Applicable	Configured Locally

Password Policy

Policy	Policy Setting	Configuration Source
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7	Default Domain Policy
Password must meet complexity requirements	True	Default Domain Policy
Relax minimum password length limits	Not Configured	Not Defined
Store passwords using reversible encryption	False	Default Domain Policy

LAPS Settings

The Local Administrator Password Solution (LAPS) provides the ability to automatically update local administrator account passwords for domain joined computers.

General Settings

Installed	True
Enabled	True
DLL File Location	C:\Program Files\LAPS\CSE\AdmPwd.dll
DLL Version	6.2.0.0

Policy Settings

Administrator Account Name	
Password Age (Days)	30
Password Length	14
Password Complexity Type	Large Letters + Small Letters + Numbers + Specials

Local Users

A local user account is available only on the computer where the local account is defined and is stored in the machine's SAM (security accounts manager) database.

Name	Description	Password Never Expires	User Cannot Change Password
Administrator	Built-in account for administering the computer/domain	True	False
DefaultAccount	A user account managed by the system.	True	False
Guest	Built-in account for guest access to the computer/domain	True	True
WDAGUtilityAccount	A user account managed and used by the system for Windows Defender Application Guard scenarios.	False	False
wu		True	False

Administrator

Provides details of this local account.

Account Details

Name	Administrator
Description	Built-in account for administering the computer/domain
Enabled	True
Password Never Expires	True
Full Name	
Security Identifier	S-1-5-21-346512116-3600583813-593958679-500
Last Login	11/26/2024 5:36:37 PM
Password Expired	False
Password Last Set	Friday, February 14, 2025 3:07:31 PM
User Cannot Change Password	False

Profile

Profile Path	
Login Script	
Home Drive	
Home Directory	

DefaultAccount

Provides details of this local account.

Account Details

Name	DefaultAccount
Description	A user account managed by the system.
Enabled	False
Password Never Expires	True
Full Name	
Security Identifier	S-1-5-21-346512116-3600583813-593958679-503
Last Login	Never
Password Expired	False
Password Last Set	Never
User Cannot Change Password	False

Profile

Profile Path	
Login Script	
Home Drive	
Home Directory	

Guest

Provides details of this local account.

Account Details

Name	Guest
Description	Built-in account for guest access to the computer/domain
Enabled	False
Password Never Expires	True
Full Name	
Security Identifier	S-1-5-21-346512116-3600583813-593958679-501
Last Login	Never
Password Expired	False
Password Last Set	Never
User Cannot Change Password	True

Profile

Profile Path	
Login Script	
Home Drive	
Home Directory	

WDAGUtilityAccount

Provides details of this local account.

Account Details

Name	WDAGUtilityAccount
Description	A user account managed and used by the system for Windows Defender Application Guard scenarios.
Enabled	False
Password Never Expires	False
Full Name	
Security Identifier	S-1-5-21-346512116-3600583813-593958679-504
Last Login	Never
Password Expired	True
Password Last Set	[Password Expired]
User Cannot Change Password	False

Profile

Profile Path	
Login Script	
Home Drive	
Home Directory	

wu

Provides details of this local account.

Account Details

Name	wu
Description	
Enabled	True
Password Never Expires	True
Full Name	wu
Security Identifier	S-1-5-21-346512116-3600583813-593958679-1002
Last Login	2/12/2025 4:41:21 PM
Password Expired	False
Password Last Set	Friday, January 3, 2025 5:06:24 PM
User Cannot Change Password	False

Profile

Profile Path	
Login Script	
Home Drive	
Home Directory	

Local Groups

A local group account is available only on the computer where the local group is defined and is stored in the machine's SAM (security accounts manager) database. It can contain both local users and domain users and groups and can be used to assign security to resources on the local machine.

Access Control Assistance Operators

Description	Members of this group can remotely query authorization attributes and permissions for resources on this computer.
Security Identifier	S-1-5-32-579
Members	

Administrators

Description	Administrators have complete and unrestricted access to the computer/domain
Security Identifier	S-1-5-32-544
Members	CONTOSO\Domain Admins XCS-2K25-DEMO\Administrator

Backup Operators

Description	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Security Identifier	S-1-5-32-551
Members	

Certificate Service DCOM Access

Description	Members of this group are allowed to connect to Certification Authorities in the enterprise
Security Identifier	S-1-5-32-574
Members	

Cryptographic Operators

Description	Members are authorized to perform cryptographic operations.
Security Identifier	S-1-5-32-569
Members	

Device Owners

Description	Members of this group can change system-wide settings.
Security Identifier	S-1-5-32-583
Members	

Distributed COM Users

Description	Members are allowed to launch, activate and use Distributed COM objects on this machine.
Security Identifier	S-1-5-32-562
Members	

Event Log Readers

Description	Members of this group can read event logs from local machine
Security Identifier	S-1-5-32-573
Members	

Guests

Description	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Security Identifier	S-1-5-32-546
Members	XCS-2K25-DEMO\Guest

Hyper-V Administrators

Description	Members of this group have complete and unrestricted access to all features of Hyper-V.
Security Identifier	S-1-5-32-578
Members	

IIS_IUSRS

Description	Built-in group used by Internet Information Services.
Security Identifier	S-1-5-32-568
Members	

Network Configuration Operators

Description	Members in this group can have some administrative privileges to manage configuration of networking features
Security Identifier	S-1-5-32-556
Members	

OpenSSH Users

Description	Members of this group may connect to this computer using SSH.
Security Identifier	S-1-5-32-585
Members	

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
Security Identifier	S-1-5-32-559
Members	

Performance Monitor Users

Description	Members of this group can access performance counter data locally and remotely
Security Identifier	S-1-5-32-558
Members	NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS

Power Users

Description	Power Users are included for backwards compatibility and possess limited administrative powers
Security Identifier	S-1-5-32-547
Members	

Print Operators

Description	Members can administer printers installed on domain controllers
Security Identifier	S-1-5-32-550
Members	

RDS Endpoint Servers

Description	Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group needs to be populated on servers running RD Connection Broker. RD Session Host servers and RD Virtualization Host servers used in the deployment need to be in this group.
Security Identifier	S-1-5-32-576
Members	

RDS Management Servers

Description	Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS Central Management service must be included in this group.
Security Identifier	S-1-5-32-577
Members	

RDS Remote Access Servers

Description	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers and RD Web Access servers used in the deployment need to be in this group.
Security Identifier	S-1-5-32-575
Members	

Remote Desktop Users

Description	Members in this group are granted the right to logon remotely
Security Identifier	S-1-5-32-555
Members	

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.
Security Identifier	S-1-5-32-580
Members	

Replicator

Description	Supports file replication in a domain
Security Identifier	S-1-5-32-552
Members	

SQLServer2005SQLBrowserUser$XCS-2K25-DEMO

Description	Members in the group have the required access and privileges to be assigned as the log on account for the associated instance of SQL Server Browser.
Security Identifier	S-1-5-21-346512116-3600583813-593958679-1001
Members	NT SERVICE\SQLBrowser

Storage Replica Administrators

Description	Members of this group have complete and unrestricted access to all features of Storage Replica.
Security Identifier	S-1-5-32-582
Members	

System Managed Accounts Group

Description	Members of this group are managed by the system.
Security Identifier	S-1-5-32-581
Members	XCS-2K25-DEMO\DefaultAccount

User Mode Hardware Operators

Description	Members of this group may operate hardware from user mode.
Security Identifier	S-1-5-32-584
Members	

Users

Description	Users are prevented from making accidental or intentional system-wide changes and can run most applications
Security Identifier	S-1-5-32-545
Members	CONTOSO\Domain Users NT AUTHORITY\Authenticated Users NT AUTHORITY\INTERACTIVE XCS-2K25-DEMO\wu

Security Options

Security Options are security policy settings that control the behavior of the local computer.

234 Security Options

Policy	Security Setting	Configuration Source
Accounts: Block Microsoft accounts	Not Defined	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Configured Locally
App Runtime: Allow Microsoft accounts to be optional	Not Defined	Not Defined
Audit Process Creation: Include command line in process creation events	Not Defined	Not Defined
Audit: Audit the access of global system objects	Disabled	Configured Locally
Audit: Audit the use of Backup and Restore privilege	Disabled	Configured Locally
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.	Not Defined	Not Defined
Audit: Shut down system immediately if unable to log security audits	Disabled	Configured Locally
AutoPlay Policies: Disallow Autoplay for non-volume devices	Not Defined	Not Defined
AutoPlay Policies: Set the default behavior for AutoRun	Not Defined	Not Defined
AutoPlay Policies: Turn off Autoplay	Not Defined	Not Defined
Biometrics: Configure enhanced anti-spoofing	Not Defined	Not Defined
Cloud Content: Turn off Microsoft consumer experiences	Not Defined	Not Defined
Connect: Require pin for pairing	Not Defined	Not Defined
Credential User Interface: Do not display the password reveal button	Not Defined	Not Defined
Credential User Interface: Enumerate administrator accounts on elevation	Not Defined	Not Defined
Credentials Delegation: Encryption Oracle Remediation	Not Defined	Not Defined
Credentials Delegation: Remote host allows delegation of non-exportable credentials	Not Defined	Not Defined
Data Collection and Preview Builds: Allow Diagnostics Data	Not Defined	Not Defined
Data Collection and Preview Builds: Do not show feedback notifications	Not Defined	Not Defined

Data Collection and Preview Builds: Toggle user control over Insider builds	Not Defined	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	Not Defined
Devices: Allow undock without having to log on	Enabled	Configured Locally
Devices: Allowed to format and eject removable media	Not Defined	Not Defined
Devices: Prevent users from installing printer drivers	Enabled	Configured Locally
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined	Not Defined
DNS Client: Turn off multicast name resolution	Not Defined	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined	Not Defined
Domain controller: LDAP server signing requirements	Not Defined	Not Defined
Domain controller: Refuse machine account password changes	Not Defined	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Configured Locally
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Configured Locally
Domain member: Digitally sign secure channel data (when possible)	Enabled	Configured Locally
Domain member: Disable machine account password changes	Enabled	Default Domain Policy
Domain member: Maximum machine account password age	30 days	Configured Locally
Domain member: Require strong (Windows 2000 or later) session key	Enabled	Configured Locally
Early Launch Antimalware: Boot-Start Driver Initialization Policy	Not Defined	Not Defined
EMET: Default Action and Mitigation Settings: Anti Detours	Not Defined	Not Defined
EMET: Default Action and Mitigation Settings: Banned Functions	Not Defined	Not Defined
EMET: Default Action and Mitigation Settings: Deep Hooks	Not Defined	Not Defined
EMET: Default Action and Mitigation Settings: Exploit Action	Not Defined	Not Defined
EMET: System ASLR	Not Defined	Not Defined
EMET: System DEP	Not Defined	Not Defined
EMET: System SEHOP	Not Defined	Not Defined

Event Log: Application: Control Event Log behavior when the log file reaches its maximum size	Not Defined	Not Defined
Event Log: Application: Specify the maximum log file size (KB)	Not Defined	Not Defined
Event Log: Security: Control Event Log behavior when the log file reaches its maximum size	Not Defined	Not Defined
Event Log: Security: Specify the maximum log file size (KB)	Not Defined	Not Defined
Event Log: Setup: Control Event Log behavior when the log file reaches its maximum size	Not Defined	Not Defined
Event Log: Setup: Specify the maximum log file size (KB)	Not Defined	Not Defined
Event Log: System: Control Event Log behavior when the log file reaches its maximum size	Not Defined	Not Defined
Event Log: System: Specify the maximum log file size (KB)	Not Defined	Not Defined
File Explorer: Enable Microsoft Defender SmartScreen	Not Defined	Not Defined
File Explorer: Microsoft Defender SmartScreen Level	Not Defined	Not Defined
File Explorer: Turn off Data Execution Prevention for Explorer	Not Defined	Not Defined
File Explorer: Turn off heap termination on corruption	Not Defined	Not Defined
File Explorer: Turn off shell protocol protected mode	Not Defined	Not Defined
Group Policy: Continue experiences on this device	Not Defined	Not Defined
Group Policy: Registry policy processing: Do not apply during periodic background processing	Not Defined	Not Defined
Group Policy: Registry policy processing: Process even if the Group Policy objects have not changed	Not Defined	Not Defined
Group Policy: Turn off background refresh of Group Policy	Not Defined	Not Defined
Interactive logon: Display user information when the session is locked	Not Defined	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Configured Locally
Interactive logon: Don't display last signed-in	Disabled	Configured Locally
Interactive logon: Machine account lockout threshold	Not Defined	Not Defined
Interactive logon: Machine inactivity limit	Not Defined	Not Defined
Interactive logon: Message text for users attempting to log on		Configured Locally
Interactive logon: Message title for users attempting to log on		Configured Locally
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	Configured Locally
Interactive logon: Prompt user to change password before expiration	5 days	Configured Locally

Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	Configured Locally
Interactive logon: Require smart card	Disabled	Configured Locally
Interactive logon: Smart card removal behavior	No Action	Configured Locally
Internet Communication settings: Turn off access to the Store	Not Defined	Not Defined
Internet Communication Settings: Turn off downloading of print drivers over HTTP	Not Defined	Not Defined
Internet Communication Settings: Turn off handwriting personalization data sharing	Not Defined	Not Defined
Internet Communication Settings: Turn off handwriting recognition error reporting	Not Defined	Not Defined
Internet Communication Settings: Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Not Defined	Not Defined
Internet Communication Settings: Turn off Internet download for Web publishing and online ordering wizards	Not Defined	Not Defined
Internet Communication Settings: Turn off printing over HTTP	Not Defined	Not Defined
Internet Communication Settings: Turn off Registration if URL connection is referring to Microsoft.com	Not Defined	Not Defined
Internet Communication Settings: Turn off Search Companion content file updates	Not Defined	Not Defined
Internet Communication Settings: Turn off the "Order Prints" picture task	Not Defined	Not Defined
Internet Communication Settings: Turn off the "Publish to Web" task for files and folders	Not Defined	Not Defined
Internet Communication Settings: Turn off the Windows Messenger Customer Experience Improvement Program	Not Defined	Not Defined
Internet Communication Settings: Turn off Windows Customer Experience Improvement Program	Not Defined	Not Defined
Internet Communication Settings: Turn off Windows Error Reporting	Not Defined	Not Defined
Internet Explorer: Disable Internet Explorer as a stand alone browser	Not Defined	Not Defined
Internet Explorer: Prevent downloading of enclosures	Not Defined	Not Defined
IPv6: Disabled Components	Not Defined	Not Defined
Lanman Workstation: Enable insecure guest logons	Not Defined	Not Defined
Locale Services: Disallow copying of user input methods to the system account for sign-in	Not Defined	Not Defined
Location and Sensors: Turn off location	Not Defined	Not Defined
Logon: Block user from showing account details on sign-in	Not Defined	Not Defined
Logon: Do not display network selection UI	Not Defined	Not Defined
Logon: Do not enumerate connected users on domain-joined computers	Not Defined	Not Defined

Logon: Enumerate local users on domain-joined computers	Not Defined	Not Defined
Logon: Turn off app notifications on the lock screen	Not Defined	Not Defined
Logon: Turn off picture password sign-in	Not Defined	Not Defined
Logon: Turn on convenience PIN sign-in	Not Defined	Not Defined
Microsoft Accounts: Block all consumer Microsoft account user authentication	Not Defined	Not Defined
Microsoft Defender Antivirus: Configure detection for potentially unwanted applications	Not Defined	Not Defined
Microsoft Defender Antivirus: Configure local setting override for reporting to Microsoft MAPS	Not Defined	Not Defined
Microsoft Defender Antivirus: Configure Watson events	Not Defined	Not Defined
Microsoft Defender Antivirus: Join Microsoft MAPS	Not Defined	Not Defined
Microsoft Defender Antivirus: Prevent users and apps from accessing dangerous websites	Not Defined	Not Defined
Microsoft Defender Antivirus: Scan removable drives	Not Defined	Not Defined
Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus	Enabled	Default Domain Policy
Microsoft Defender Antivirus: Turn on behavior monitoring	Not Defined	Not Defined
Microsoft Defender Antivirus: Turn on e-mail scanning	Not Defined	Not Defined
Microsoft network client: Digitally sign communications (always)	Not Defined	Not Defined
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Configured Locally
Microsoft network client: Enable SMB version 1 protocol	Disabled	Configured Locally
Microsoft network client: Send unencrypted password to connect to third-party SMB servers	Disabled	Configured Locally
Microsoft network server: Amount of idle time required before suspending a session	15 minutes	Configured Locally
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined	Not Defined
Microsoft network server: Digitally sign communications (always)	Not Defined	Not Defined
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	Configured Locally
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Configured Locally
Microsoft network server: Enable SMB version 1 protocol	Not Defined	Not Defined
Microsoft network server: Enable SMB version 2 protocol	Not Defined	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined	Not Defined

Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider	Not Defined	Not Defined
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Disabled	Configured Locally
MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	Not Defined	Not Defined
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Not Defined	Not Defined
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Enabled	Configured Locally
MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	Not Defined	Not Defined
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Not Defined	Not Defined
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	Not Defined	Not Defined
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	Not Defined	Not Defined
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	Not Defined	Not Defined
MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted	Not Defined	Not Defined
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted	Not Defined	Not Defined
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	Not Defined	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain Policy
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Configured Locally
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	Configured Locally
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled	Configured Locally
Network access: Let Everyone permissions apply to anonymous users	Disabled	Configured Locally
Network access: Named pipes that can be accessed anonymously		Configured Locally
Network access: Remotely accessible registry paths	Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications	Configured Locally
Network access: Remotely accessible registry paths and subpaths	Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Perflib Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Control\Terminal	Configured Locally

	Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\SysmonLog	
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Configured Locally
Network access: Restrict clients allowed to make remote calls to SAM	Not Defined	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	Configured Locally
Network Connections: Prohibit installation and configuration of Network Bridge on your DNS domain network	Not Defined	Not Defined
Network Connections: Prohibit use of Internet Connection Sharing on your DNS domain network	Not Defined	Not Defined
Network Connections: Require domain users to elevate when setting a network's location	Not Defined	Not Defined
Network Provider: Hardened UNC Paths		Configured Locally
Network security: Allow Local System to use computer identity for NTLM	Not Defined	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined	Not Defined
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Not Defined	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled	Default Domain Policy
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy
Network security: LAN Manager authentication level	Not Defined	Not Defined
Network security: LDAP client signing requirements	Negotiate Signing	Configured Locally
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption	Configured Locally
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encryption	Configured Locally
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined	Not Defined

Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined	Not Defined
OneDrive: Prevent the usage of OneDrive for file storage	Not Defined	Not Defined
Personalization: Prevent enabling lock screen camera	Not Defined	Not Defined
Personalization: Prevent enabling lock screen slide show	Not Defined	Not Defined
Recovery console: Allow automatic administrative logon	Disabled	Configured Locally
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	Configured Locally
Regional and Language Options: Allow users to enable online speech recognition services	Not Defined	Not Defined
Remote Assistance: Allow Offer Remote Assistance	Not Defined	Not Defined
Remote Assistance: Allow Solicited Remote Assistance	Not Defined	Not Defined
Remote Desktop Connection Client: Do not allow passwords to be saved	Not Defined	Not Defined
Remote Procedure Call: Enable RPC Endpoint Mapper Client Authentication	Not Defined	Not Defined
Remote Procedure Call: Restrict Unauthenticated RPC clients	Not Defined	Not Defined
Search: Allow Cloud Search	Not Defined	Not Defined
Search: Allow indexing of encrypted files	Not Defined	Not Defined
Secure Channel: Enable SSL 3.0 (Client)	Not Defined	Not Defined
Secure Channel: Enable SSL 3.0 (Server)	Not Defined	Not Defined
Secure Channel: Enable TLS 1.0 (Client)	Not Defined	Not Defined
Secure Channel: Enable TLS 1.0 (Server)	Not Defined	Not Defined
Secure Channel: Enable TLS 1.1 (Client)	Not Defined	Not Defined
Secure Channel: Enable TLS 1.1 (Server)	Not Defined	Not Defined
Secure Channel: Enable TLS 1.2 (Client)	Not Defined	Not Defined
Secure Channel: Enable TLS 1.2 (Server)	Not Defined	Not Defined
Security Providers: WDigest Authentication	Not Defined	Not Defined
Shutdown: Allow system to be shut down without having to log on	Disabled	Configured Locally

Shutdown: Clear virtual memory pagefile	Disabled	Configured Locally
Sleep Settings: Require a password when a computer wakes (on battery)	Not Defined	Not Defined
Sleep Settings: Require a password when a computer wakes (plugged in)	Not Defined	Not Defined
System Cryptography: Force strong key protection for user keys stored on the computer	Not Defined	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	Configured Locally
System objects: Require case insensitivity for non-Windows subsystems	Enabled	Configured Locally
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Configured Locally
System settings: Optional subsystems		Configured Locally
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	Configured Locally
TCP/IP: NetBT NodeType	Not Defined	Not Defined
Turn off Microsoft Peer-to-Peer Networking Services	Not Defined	Not Defined
Turn on Mapper I/O (LLTDIO) driver	Not Defined	Not Defined
Turn on Responder (RSPNDR) driver	Not Defined	Not Defined
User Account Control: Admin Approval Mode for the built-in Administrator account	Not Defined	Not Defined
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	Configured Locally
User Account Control: Apply UAC restrictions to local accounts on network logons	Not Defined	Not Defined
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries	Configured Locally
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials	Configured Locally
User Account Control: Detect application installations and prompt for elevation	Enabled	Configured Locally
User Account Control: Only elevate executables that are signed and validated	Disabled	Configured Locally
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	Configured Locally
User Account Control: Run all administrators in Admin approval mode	Enabled	Configured Locally
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled	Configured Locally
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled	Configured Locally
Windows Connect Now: Configuration of wireless settings using Windows Connect Now	Not Defined	Not Defined
Windows Connect Now: Prohibit access of the Windows Connect Now wizards	Not Defined	Not Defined

Windows Connection Manager: Minimize the number of simultaneous connections to the Internet or a Windows Domain	Not Defined	Not Defined
Windows Connection Manager: Prohibit connection to non-domain networks when connected to domain authenticated network	Not Defined	Not Defined
Windows Ink Workspace: Allow Windows Ink Workspace	Not Defined	Not Defined
Windows Installer: Allow user control over installs	Not Defined	Not Defined
Windows Installer: Always install with elevated privileges	Not Defined	Not Defined
Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts	Not Defined	Not Defined
Windows Logon Options: Sign-in and lock last interactive user automatically after a restart	Disabled	Configured Locally
Windows Performance PerfTrack: Enable/Disable PerfTrack	Not Defined	Not Defined
Windows PowerShell: Turn on PowerShell Script Block Logging	Not Defined	Not Defined
Windows PowerShell: Turn on PowerShell Transcription	Not Defined	Not Defined
Windows Security: App and browser protection: Prevent users from modifying settings	Not Defined	Not Defined
Windows Update: Defer feature updates	Not Defined	Not Defined
Windows Update: Defer quality updates	Not Defined	Not Defined
Windows Update: Manage preview builds	Not Defined	Not Defined
Windows Update: Manage preview builds (Branch Readiness Level)	Not Defined	Not Defined

User Rights Assignment

User Rights Assignment covers both the privileges and user rights that have been assigned to user accounts. Privileges determine the type of system operations that a user account can perform whereas account rights determine the type of logon that a user account can perform - for example logon as a service.

44 User Rights

Display Name	Name	Configuration Source	Account Names
Access Credential Manager as a trusted caller	SeTrustedCredManAccessPrivilege	Configured Locally	
Access this computer from the network	SeNetworkLogonRight	Configured Locally	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Users Everyone
Act as part of the operating system	SeTcbPrivilege	Configured Locally	
Add workstations to domain	SeMachineAccountPrivilege	Configured Locally	
Adjust memory quotas for a process	SeIncreaseQuotaPrivilege	Configured Locally	BUILTIN\Administrators IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS
Allow log on locally	SeInteractiveLogonRight	Configured Locally	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Users
Allow log on through Remote Desktop Services	SeRemoteInteractiveLogonRight	Configured Locally	BUILTIN\Administrators BUILTIN\Remote Desktop Users
Back up files and directories	SeBackupPrivilege	Configured Locally	BUILTIN\Administrators BUILTIN\Backup Operators
Bypass traverse checking	SeChangeNotifyPrivilege	Configured Locally	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Users Everyone NT AUTHORITY\LOCAL SERVICE

			NT AUTHORITY\NETWORK SERVICE NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS
Change the system time	SeSystemtimePrivilege	Configured Locally	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE
Change the time zone	SeTimeZonePrivilege	Configured Locally	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE
Create a pagefile	SeCreatePagefilePrivilege	Configured Locally	BUILTIN\Administrators
Create a token object	SeCreateTokenPrivilege	Configured Locally	
Create global objects	SeCreateGlobalPrivilege	Configured Locally	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE
Create permanent shared objects	SeCreatePermanentPrivilege	Configured Locally	
Create symbolic links	SeCreateSymbolicLinkPrivilege	Configured Locally	BUILTIN\Administrators
Debug programs	SeDebugPrivilege	Configured Locally	BUILTIN\Administrators
Deny access to this computer from the network	SeDenyNetworkLogonRight	Configured Locally	
Deny log on as a batch job	SeDenyBatchLogonRight	Configured Locally	
Deny log on as a service	SeDenyServiceLogonRight	Configured Locally	
Deny log on locally	SeDenyInteractiveLogonRight	Configured Locally	
Deny log on through Remote Desktop Services	SeDenyRemoteInteractiveLogonRight	Configured Locally	
Enable computer and user accounts to be trusted for delegation	SeEnableDelegationPrivilege	Configured Locally	
Force shutdown from a remote system	SeRemoteShutdownPrivilege	Configured Locally	BUILTIN\Administrators
Generate security audits	SeAuditPrivilege	Configured Locally	IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE

Impersonate a client after authentication	SeImpersonatePrivilege	Configured Locally	BUILTIN\Administrators BUILTIN\IIS_IUSRS NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE S-1-5-99-216390572-1995538116-3857911515-2404958512-2623887229
Increase a process working set	SeIncreaseWorkingSetPrivilege	Configured Locally	BUILTIN\Users
Increase scheduling priority	SeIncreaseBasePriorityPrivilege	Configured Locally	BUILTIN\Administrators Window Manager\Window Manager Group
Load and unload device drivers	SeLoadDriverPrivilege	Configured Locally	BUILTIN\Administrators
Lock pages in memory	SeLockMemoryPrivilege	Configured Locally	
Log on as a batch job	SeBatchLogonRight	Configured Locally	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\IIS_IUSRS BUILTIN\Performance Log Users
Log on as a service	SeServiceLogonRight	Configured Locally	CONTOSO\sysadmin IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\NETWORK SERVICE NT SERVICE\ALL SERVICES NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS NT SERVICE\SQLTELEMETRY$SQLEXPRESS RESTRICTED SERVICES\ALL RESTRICTED SERVICES XCS-2K25-DEMO\SQLServer2005SQLBrowserUser$XCS-2K25-DEMO XCS-2K25-DEMO\wu
Manage auditing and security log	SeSecurityPrivilege	Configured Locally	BUILTIN\Administrators
Modify an object label	SeRelabelPrivilege	Configured Locally	
Modify firmware environment values	SeSystemEnvironmentPrivilege	Configured Locally	BUILTIN\Administrators
Perform volume maintenance tasks	SeManageVolumePrivilege	Configured Locally	BUILTIN\Administrators NT SERVICE\MSSQL$SQLEXPRESS
Profile single process	SeProfileSingleProcessPrivilege	Configured Locally	BUILTIN\Administrators
Profile system performance	SeSystemProfilePrivilege	Configured Locally	BUILTIN\Administrators NT SERVICE\WdiServiceHost
Remove computer from docking station	SeUndockPrivilege	Configured	BUILTIN\Administrators

		Locally	
Replace a process-level token	SeAssignPrimaryTokenPrivilege	Configured Locally	IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS
Restore files and directories	SeRestorePrivilege	Configured Locally	BUILTIN\Administrators BUILTIN\Backup Operators
Shut down the system	SeShutdownPrivilege	Configured Locally	BUILTIN\Administrators BUILTIN\Backup Operators
Synchronize directory service data	SeSyncAgentPrivilege	Configured Locally	
Take ownership of files or other objects	SeTakeOwnershipPrivilege	Configured Locally	BUILTIN\Administrators

Windows Firewall

Windows Firewall with Advanced Security is a stateful firewall integrated into Windows operating systems which blocks unauthorized network traffic flowing into or out of the local computer.

General Settings

Active Profile	Domain

Firewall Profiles

Name	State
Domain Profile	On (recommended)
Private Profile	On (recommended)
Public Profile	On (recommended)

Domain Profile

The domain profile applies to networks where the host system can authenticate to a domain controller.

Firewall State

Setting	Value	Configuration Source
Firewall State	On (recommended)	Local
Default Inbound Action	Block (default)	Local
Default Outbound Action	Allow (default)	Local

Network Interfaces

Excluded Interfaces	

Settings

Display Notification	False
Allow Unicast Response	True
Apply Local Firewall Rules	True
Apply Local Connection Security Rules	True

Logging Settings

Log File Path	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
Log File Size Limit	4,096 KB
Log Dropped Packets	False
Log Successful Connections	False

Private Profile

The private profile is a user-assigned profile and is used to designate private or home networks.

Firewall State

Setting	Value	Configuration Source
Firewall State	On (recommended)	Local
Default Inbound Action	Block (default)	Local
Default Outbound Action	Allow (default)	Local

Network Interfaces

Excluded Interfaces	

Settings

Display Notification	False
Allow Unicast Response	True
Apply Local Firewall Rules	True
Apply Local Connection Security Rules	True

Logging Settings

Log File Path	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
Log File Size Limit	4,096 KB
Log Dropped Packets	False
Log Successful Connections	False

Public Profile

The public profile is used to designate public networks such as Wi-Fi hotspots at coffee shops, airports, and other locations.

Firewall State

Setting	Value	Configuration Source
Firewall State	On (recommended)	Local
Default Inbound Action	Block (default)	Local
Default Outbound Action	Allow (default)	Local

Network Interfaces

Excluded Interfaces	

Settings

Display Notification	False
Allow Unicast Response	True
Apply Local Firewall Rules	True
Apply Local Connection Security Rules	True

Logging Settings

Log File Path	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
Log File Size Limit	4,096 KB
Log Dropped Packets	False
Log Successful Connections	False

Inbound Rules

Inbound rules determine what action should be taken by the firewall when inspecting traffic coming into the machine from external sources. Only enabled rules are displayed.

74 Windows Firewall Rules

Rule Name	Profile Names	Protocol	Local Addresses	Local Ports	Remote Addresses	Remote Ports
@{MicrosoftWindows.LKG.Search_1000.26100.1742.0_x64__cw5n1h2txyewy?ms-res...	Domain, Private	Any	Any	Any	Any	Any
AllJoyn Router (TCP-In)	Domain, Private	TCP	Any	9955	Any	Any
AllJoyn Router (UDP-In)	Domain, Private	UDP	Any	Any	Any	Any
App Installer	Domain, Private	Any	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP-In)	Private, Public	TCP	Any	2177	PlayToDevice	Any
Cast to Device functionality (qWave-UDP-In)	Private, Public	UDP	Any	2177	PlayToDevice	Any
Cast to Device SSDP Discovery (UDP-In)	Public	UDP	Any	PlayToDiscovery	Any	Any
Cast to Device streaming server (HTTP-Streaming-In)	Private	TCP	Any	10246	LocalSubnet	Any
Cast to Device streaming server (HTTP-Streaming-In)	Domain	TCP	Any	10246	Any	Any
Cast to Device streaming server (HTTP-Streaming-In)	Public	TCP	Any	10246	PlayToDevice	Any
Cast to Device streaming server (RTCP-Streaming-In)	Private	UDP	Any	Any	LocalSubnet	Any
Cast to Device streaming server (RTCP-Streaming-In)	Public	UDP	Any	Any	PlayToDevice	Any
Cast to Device streaming server (RTCP-Streaming-In)	Domain	UDP	Any	Any	Any	Any
Cast to Device streaming server (RTSP-Streaming-In)	Domain	TCP	Any	23554 23555 23556	Any	Any
Cast to Device streaming server (RTSP-Streaming-In)	Public	TCP	Any	23554 23555 23556	PlayToDevice	Any
Cast to Device streaming server (RTSP-Streaming-In)	Private	TCP	Any	23554 23555 23556	LocalSubnet	Any
Cast to Device UPnP Events (TCP-In)	Public	TCP	Any	2869	PlayToDevice	Any

Core Networking - Destination Unreachable (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)	Any	ICMPv4	Any	RPC	Any	Any
Core Networking - Dynamic Host Configuration Protocol (DHCP-In)	Any	UDP	Any	68	Any	67
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)	Any	UDP	Any	546	Any	547
Core Networking - Internet Group Management Protocol (IGMP-In)	Any	2	Any	Any	Any	Any
Core Networking - IPHTTPS (TCP-In)	Any	TCP	Any	IPHTTPSIn	Any	Any
Core Networking - IPv6 (IPv6-In)	Any	41	Any	Any	Any	Any
Core Networking - Multicast Listener Done (ICMPv6-In)	Any	ICMPv6	Any	RPC	LocalSubnet6	Any
Core Networking - Multicast Listener Query (ICMPv6-In)	Any	ICMPv6	Any	RPC	LocalSubnet6	Any
Core Networking - Multicast Listener Report (ICMPv6-In)	Any	ICMPv6	Any	RPC	LocalSubnet6	Any
Core Networking - Multicast Listener Report v2 (ICMPv6-In)	Any	ICMPv6	Any	RPC	LocalSubnet6	Any
Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Packet Too Big (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Parameter Problem (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Router Advertisement (ICMPv6-In)	Any	ICMPv6	Any	RPC	fe80::/64	Any
Core Networking - Router Solicitation (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Teredo (UDP-In)	Any	UDP	Any	Teredo	Any	Any
Core Networking - Time Exceeded (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
Delivery Optimization (TCP-In)	Any	TCP	Any	7680	Any	Any
Delivery Optimization (UDP-In)	Any	UDP	Any	7680	Any	Any
Desktop App Web Viewer	Domain, Private, Public	Any	Any	Any	Any	Any
DFS Management (DCOM-In)	Any	TCP	Any	135	Any	Any
DFS Management (SMB-In)	Any	TCP	Any	445	Any	Any
DFS Management (TCP-In)	Any	TCP	Any	RPC	Any	Any
DFS Management (WMI-In)	Any	TCP	Any	RPC	Any	Any
DIAL protocol server (HTTP-In)	Domain	TCP	Any	10247	Any	Any

DIAL protocol server (HTTP-In)	Private	TCP	Any	10247	LocalSubnet	Any
Feedback Hub	Domain, Private	Any	Any	Any	Any	Any
Google Chrome (mDNS-In)	Any	UDP	Any	5353	Any	Any
mDNS (UDP-In)	Domain	UDP	Any	5353	Any	Any
mDNS (UDP-In)	Public	UDP	Any	5353	LocalSubnet	Any
mDNS (UDP-In)	Private	UDP	Any	5353	LocalSubnet	Any
Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
Microsoft Media Foundation Network Source IN [TCP 554]	Any	TCP	Any	554 8554-8558	LocalSubnet	Any
Microsoft Media Foundation Network Source IN [UDP 5004-5009]	Any	UDP	Any	5000-5020	LocalSubnet	Any
OpenSSH SSH Server (sshd)	Private	TCP	Any	22	Any	Any
Start	Domain, Private	Any	Any	Any	Any	Any
Web Management Service (HTTP Traffic-In)	Any	TCP	Any	8172	Any	Any
WFD ASP Coordination Protocol (UDP-In)	Any	UDP	Any	7235	LocalSubnet	7235
WFD Driver-only (TCP-In)	Any	TCP	Any	Any	Any	Any
WFD Driver-only (UDP-In)	Any	UDP	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private	Any	Any	Any	Any	Any
Windows Remote Management (HTTP-In)	Domain, Private	TCP	Any	5985	Any	Any
Windows Remote Management (HTTP-In)	Public	TCP	Any	5985	LocalSubnet	Any
Windows Security	Domain, Private	Any	Any	Any	Any	Any
Wireless Display (TCP-In)	Any	TCP	Any	Any	Any	Any
Wireless Display Infrastructure Back Channel (TCP-In)	Any	TCP	Any	7250	Any	Any
Work or school account	Domain, Private	Any	Any	Any	Any	Any
World Wide Web Services (HTTP Traffic-In)	Any	TCP	Any	80	Any	Any

World Wide Web Services (HTTPS Traffic-In)	Any	TCP	Any	443	Any	Any
World Wide Web Services (QUIC Traffic-In)	Any	UDP	Any	443	Any	Any
Your account	Domain, Private	Any	Any	Any	Any	Any

@{MicrosoftWindows.LKG.Search_1000.26100.1742.0_x64__cw5n1h2txyewy?ms-resource...

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	@{MicrosoftWindows.LKG.Search_1000.26100.1742.0_x64__cw5n1h2txyewy?ms-resource:/ /MicrosoftWindows.LKG.Search/Resources/ProductPkgDisplayName}
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

AllJoyn Router (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for AllJoyn Router traffic [TCP]
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	9955
Remote Ports	Any

AllJoyn Router (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for AllJoyn Router traffic [UDP]
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

App Installer

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	App Installer
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Cast to Device functionality (qWave-TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [TCP 2177]
Direction	Inbound
Enabled	True
Profile Names	Private, Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	2177
Remote Ports	Any

Cast to Device functionality (qWave-UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [UDP 2177]
Direction	Inbound
Enabled	True
Profile Names	Private, Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	2177
Remote Ports	Any

Cast to Device SSDP Discovery (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule to allow discovery of Cast to Device targets using SSDP
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	PlayToDiscovery
Remote Ports	Any

Cast to Device streaming server (HTTP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using HTTP. [TCP 10246]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	10246
Remote Ports	Any

Cast to Device streaming server (HTTP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using HTTP. [TCP 10246]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	10246
Remote Ports	Any

Cast to Device streaming server (HTTP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using HTTP. [TCP 10246]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	10246
Remote Ports	Any

Cast to Device streaming server (RTCP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Cast to Device streaming server (RTCP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Cast to Device streaming server (RTCP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings	
Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope	
Local Addresses	Any
Remote Addresses	Any

Programs And Services	
Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports	
Protocol	UDP
Local Ports	Any
Remote Ports	Any

Cast to Device streaming server (RTSP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [TCP 23554, 23555, 23556]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports

Protocol	TCP
Local Ports	23554 23555 23556
Remote Ports	Any

Cast to Device streaming server (RTSP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [TCP 23554, 23555, 23556]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports

Protocol	TCP
Local Ports	23554 23555 23556
Remote Ports	Any

Cast to Device streaming server (RTSP-Streaming-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [TCP 23554, 23555, 23556]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports

Protocol	TCP
Local Ports	23554 23555 23556
Remote Ports	Any

Cast to Device UPnP Events (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule to allow receiving UPnP Events from Cast to Device targets
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	2869
Remote Ports	Any

Core Networking - Destination Unreachable (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Destination Unreachable error messages are sent from any node that a packet traverses which is unable to forward the packet for any reason except congestion.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Destination Unreachable Fragmentation Needed error messages are sent from any node that a packet traverses which is unable to forward the packet because fragmentation was needed and the don't fragment bit was set.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv4
Local Ports	RPC
Remote Ports	Any

Core Networking - Dynamic Host Configuration Protocol (DHCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	68
Remote Ports	67

Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Allows DHCPV6 (Dynamic Host Configuration Protocol for IPv6) messages for stateful and stateless configuration.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	546
Remote Ports	547

Core Networking - Internet Group Management Protocol (IGMP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	IGMP messages are sent and received by nodes to create, join and depart multicast groups.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	2
Local Ports	Any
Remote Ports	Any

Core Networking - IPHTTPS (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound TCP rule to allow IPHTTPS tunneling technology to provide connectivity across HTTP proxies and firewalls.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	IPHTTPSIn
Remote Ports	Any

Core Networking - IPv6 (IPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunneling services.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	41
Local Ports	Any
Remote Ports	Any

Core Networking - Multicast Listener Done (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Multicast Listener Done messages inform local routers that there are no longer any members remaining for a specific multicast address on the subnet.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Query (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	An IPv6 multicast-capable router uses the Multicast Listener Query message to query a link for multicast group membership.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Report (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Report v2 (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Multicast Listener Report v2 message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Neighbor Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Neighbor Discovery Solicitations are sent by nodes to discover the link-layer address of another on-link IPv6 node.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Packet Too Big (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Packet Too Big error messages are sent from any node that a packet traverses which is unable to forward the packet because the packet is too large for the next link.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Parameter Problem (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Parameter Problem error messages are sent by nodes as a result of incorrectly generated packets.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Router Advertisement (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Router Advertisement messages are sent by routers to other nodes for stateless auto-configuration.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	fe80::/64

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Router Solicitation (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Router Solicitation messages are sent by nodes seeking routers to provide stateless auto-configuration.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Teredo (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound UDP rule to allow Teredo edge traversal, a technology that provides address assignment and automatic tunneling for unicast IPv6 traffic when an IPv6/IPv4 host is located behind an IPv4 network address translator.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Teredo
Remote Ports	Any

Core Networking - Time Exceeded (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Time Exceeded error messages are generated from any node that a packet traverses if the Hop Limit value is decremented to zero at any point on the path.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Delivery Optimization (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule to allow Delivery Optimization to connect to remote endpoints
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	7680
Remote Ports	Any

Delivery Optimization (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule to allow Delivery Optimization to connect to remote endpoints
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	7680
Remote Ports	Any

Desktop App Web Viewer

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Desktop App Web Viewer
Direction	Inbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

DFS Management (DCOM-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for DFS Management to allow remote DCOM activation via the RPCSS service.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	135
Remote Ports	Any

DFS Management (SMB-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for DFS Management to allow Server Message Block transmission and reception via Named Pipes. [TCP 445].
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	445
Remote Ports	Any

DFS Management (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for DFS Management to allow the DFS Management service to be remotely managed via DCOM.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\dfsfrsHost.exe

Protocols and Ports

Protocol	TCP
Local Ports	RPC
Remote Ports	Any

DFS Management (WMI-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for DFS Management to allow remote invocation of WMI.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	RPC
Remote Ports	Any

DIAL protocol server (HTTP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for DIAL protocol server to allow remote control of Apps using HTTP. [TCP 10247]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	10247
Remote Ports	Any

DIAL protocol server (HTTP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for DIAL protocol server to allow remote control of Apps using HTTP. [TCP 10247]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	10247
Remote Ports	Any

Feedback Hub

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Feedback Hub
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Google Chrome (mDNS-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for Google Chrome to allow mDNS traffic.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\Program Files\Google\Chrome\Application\chrome.exe

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

mDNS (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for mDNS traffic [UDP]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

mDNS (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for mDNS traffic [UDP]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

mDNS (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for mDNS traffic [UDP]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

Microsoft Edge (mDNS-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for Microsoft Edge to allow mDNS traffic.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

Microsoft Edge (mDNS-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for Microsoft Edge to allow mDNS traffic.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\133.0.3065.59\msedgewebview2.exe

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

Microsoft Media Foundation Network Source IN [TCP 554]

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	InBound Rule for the Microsoft Media Foundation's Capture SVC to open TCP port to enable RTSP
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	554 8554-8558
Remote Ports	Any

Microsoft Media Foundation Network Source IN [UDP 5004-5009]

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	InBound Rule for the Microsoft Media Foundation's Capture SVC to open UDP port to enable RTSP
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	5000-5020
Remote Ports	Any

OpenSSH SSH Server (sshd)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for OpenSSH SSH Server (sshd)
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\OpenSSH\sshd.exe

Protocols and Ports

Protocol	TCP
Local Ports	22
Remote Ports	Any

Start

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Start
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Web Management Service (HTTP Traffic-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	An inbound rule to allow Web Management Service traffic for Internet Information Services (IIS) [TCP 8172]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	system

Protocols and Ports

Protocol	TCP
Local Ports	8172
Remote Ports	Any

WFD ASP Coordination Protocol (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for WLAN Service to allow coordination protocol for WFD Service sessions [UDP 7235]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	7235
Remote Ports	7235

WFD Driver-only (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for drivers to communicate over WFD (TCP-In)
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

WFD Driver-only (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for drivers to communicate over WFD (UDP-In)
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Remote Management (HTTP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for Windows Remote Management via WS-Management. [TCP 5985]
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	5985
Remote Ports	Any

Windows Remote Management (HTTP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for Windows Remote Management via WS-Management. [TCP 5985]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	5985
Remote Ports	Any

Windows Security

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Security
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Wireless Display (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for Wireless Display [TCP]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\WUDFHost.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Wireless Display Infrastructure Back Channel (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for Wireless Display Infrastructure back channel [TCP]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\CastSrv.exe

Protocols and Ports

Protocol	TCP
Local Ports	7250
Remote Ports	Any

Work or school account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Work or school account
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

World Wide Web Services (HTTP Traffic-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	An inbound rule to allow HTTP traffic for Internet Information Services (IIS) [TCP 80]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	80
Remote Ports	Any

World Wide Web Services (HTTPS Traffic-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	An inbound rule to allow HTTPS traffic for Internet Information Services (IIS) [TCP 443]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	443
Remote Ports	Any

World Wide Web Services (QUIC Traffic-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	An inbound rule to allow QUIC traffic for Internet Information Services (IIS) [UDP 443]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	UDP
Local Ports	443
Remote Ports	Any

Your account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Your account
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Outbound Rules

Outbound rules determine what action should be taken by the firewall when inspecting traffic coming from the machine going to external sources. Only enabled rules are displayed.

69 Windows Firewall Rules

Rule Name	Profile Names	Protocol	Local Addresses	Local Ports	Remote Addresses	Remote Ports
@{MicrosoftWindows.LKG.Search_1000.26100.1742.0_x64__cw5n1h2txyewy?ms-res...	Domain, Private, Public	Any	Any	Any	Any	Any
AllJoyn Router (TCP-Out)	Domain, Private	TCP	Any	Any	Any	Any
AllJoyn Router (UDP-Out)	Domain, Private	UDP	Any	Any	Any	Any
App Installer	Domain, Private, Public	Any	Any	Any	Any	Any
Captive Portal Flow	Domain, Private, Public	Any	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP-Out)	Private, Public	TCP	Any	Any	PlayToDevice	2177
Cast to Device functionality (qWave-UDP-Out)	Private, Public	UDP	Any	Any	PlayToDevice	2177
Cast to Device streaming server (RTP-Streaming-Out)	Public	UDP	Any	Any	PlayToDevice	Any
Cast to Device streaming server (RTP-Streaming-Out)	Domain	UDP	Any	Any	Any	Any
Cast to Device streaming server (RTP-Streaming-Out)	Private	UDP	Any	Any	LocalSubnet	Any
Connected User Experiences and Telemetry	Any	TCP	Any	Any	Any	443
Core Networking - DNS (UDP-Out)	Any	UDP	Any	Any	Any	53
Core Networking - Dynamic Host Configuration Protocol (DHCP-Out)	Any	UDP	Any	68	Any	67
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)	Any	UDP	Any	546	Any	547
Core Networking - Group Policy (LSASS-Out)	Domain	TCP	Any	Any	Any	Any

Core Networking - Group Policy (NP-Out)	Domain	TCP	Any	Any	Any	445
Core Networking - Group Policy (TCP-Out)	Domain	TCP	Any	Any	Any	Any
Core Networking - Internet Group Management Protocol (IGMP-Out)	Any	2	Any	Any	Any	Any
Core Networking - IPHTTPS (TCP-Out)	Any	TCP	Any	Any	Any	IPHTTPSOut
Core Networking - IPv6 (IPv6-Out)	Any	41	Any	Any	Any	Any
Core Networking - Multicast Listener Done (ICMPv6-Out)	Any	ICMPv6	Any	RPC	LocalSubnet6	Any
Core Networking - Multicast Listener Query (ICMPv6-Out)	Any	ICMPv6	Any	RPC	LocalSubnet6	Any
Core Networking - Multicast Listener Report (ICMPv6-Out)	Any	ICMPv6	Any	RPC	LocalSubnet6	Any
Core Networking - Multicast Listener Report v2 (ICMPv6-Out)	Any	ICMPv6	Any	RPC	LocalSubnet6	Any
Core Networking - Neighbor Discovery Advertisement (ICMPv6-Out)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Neighbor Discovery Solicitation (ICMPv6-Out)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Packet Too Big (ICMPv6-Out)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Parameter Problem (ICMPv6-Out)	Any	ICMPv6	Any	RPC	Any	Any
Core Networking - Router Advertisement (ICMPv6-Out)	Any	ICMPv6	fe80::/64	RPC	LocalSubnet6 ff02::1 fe80::/64	Any
Core Networking - Router Solicitation (ICMPv6-Out)	Any	ICMPv6	Any	RPC	LocalSubnet6 ff02::2 fe80::/64	Any
Core Networking - Teredo (UDP-Out)	Any	UDP	Any	Any	Any	Any
Core Networking - Time Exceeded (ICMPv6-Out)	Any	ICMPv6	Any	RPC	Any	Any
Desktop App Web Viewer	Domain, Private, Public	Any	Any	Any	Any	Any
Email and accounts	Domain, Private, Public	Any	Any	Any	Any	Any
Feedback Hub	Domain, Private, Public	Any	Any	Any	Any	Any
mDNS (UDP-Out)	Domain	UDP	Any	Any	Any	5353
mDNS (UDP-Out)	Public	UDP	Any	Any	LocalSubnet	5353
mDNS (UDP-Out)	Private	UDP	Any	Any	LocalSubnet	5353

Microsoft Media Foundation Network Source OUT [TCP ALL]	Any	TCP	Any	Any	LocalSubnet	554 8554-8558
Narrator	Domain, Private, Public	Any	Any	Any	Any	Any
Start	Domain, Private, Public	Any	Any	Any	Any	Any
WFD ASP Coordination Protocol (UDP-Out)	Any	UDP	Any	7235	LocalSubnet	7235
WFD Driver-only (TCP-Out)	Any	TCP	Any	Any	Any	Any
WFD Driver-only (UDP-Out)	Any	UDP	Any	Any	Any	Any
Windows Default Lock Screen	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Defender SmartScreen	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Device Management Certificate Installer (TCP out)	Any	TCP	Any	49152-65535	Any	Any
Windows Device Management Device Enroller (TCP out)	Any	TCP	Any	49152-65535	Any	80 443
Windows Device Management Enrollment Service (TCP out)	Any	TCP	Any	49152-65535	Any	Any
Windows Device Management Sync Client (TCP out)	Any	TCP	Any	49152-65535	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private,	Any	Any	Any	Any	Any

	Public					
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Print	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Security	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Shell Experience	Domain, Private, Public	Any	Any	Any	Any	Any
Windows Terminal	Domain, Private, Public	Any	Any	Any	Any	Any
Wireless Display (TCP-Out)	Any	TCP	Any	Any	Any	Any
Wireless Display (UDP-Out)	Any	UDP	Any	Any	Any	Any
Work or school account	Domain, Private, Public	Any	Any	Any	Any	Any
Your account	Domain, Private, Public	Any	Any	Any	Any	Any

@{MicrosoftWindows.LKG.Search_1000.26100.1742.0_x64__cw5n1h2txyewy?ms-resource...

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	@{MicrosoftWindows.LKG.Search_1000.26100.1742.0_x64__cw5n1h2txyewy?ms-resource:/ /MicrosoftWindows.LKG.Search/Resources/ProductPkgDisplayName}
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

AllJoyn Router (TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for AllJoyn Router traffic [TCP]
Direction	Outbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

AllJoyn Router (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for AllJoyn Router traffic [UDP]
Direction	Outbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

App Installer

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	App Installer
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Captive Portal Flow

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Captive Portal Flow
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Cast to Device functionality (qWave-TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [TCP 2177]
Direction	Outbound
Enabled	True
Profile Names	Private, Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	2177

Cast to Device functionality (qWave-UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [UDP 2177]
Direction	Outbound
Enabled	True
Profile Names	Private, Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	2177

Cast to Device streaming server (RTP-Streaming-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Outbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Programs And Services

Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Cast to Device streaming server (RTP-Streaming-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Cast to Device streaming server (RTP-Streaming-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\mdeserver.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Connected User Experiences and Telemetry

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Unified Telemetry Client Outbound Traffic
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	443

Core Networking - DNS (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule to allow DNS requests. DNS responses based on requests that matched this rule will be permitted regardless of source address. This behavior is classified as loose source mapping. [LSM] [UDP 53]
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	53

Core Networking - Dynamic Host Configuration Protocol (DHCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	68
Remote Ports	67

Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Allows DHCPV6 (Dynamic Host Configuration Protocol for IPv6) messages for stateful and stateless configuration.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	546
Remote Ports	547

Core Networking - Group Policy (LSASS-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule to allow remote LSASS traffic for Group Policy updates [TCP].
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\lsass.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Core Networking - Group Policy (NP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Core Networking - Group Policy (NP-Out)
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	445

Core Networking - Group Policy (TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule to allow remote RPC traffic for Group Policy updates. [TCP]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Core Networking - Internet Group Management Protocol (IGMP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	IGMP messages are sent and received by nodes to create, join and depart multicast groups.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	2
Local Ports	Any
Remote Ports	Any

Core Networking - IPHTTPS (TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound TCP rule to allow IPHTTPS tunneling technology to provide connectivity across HTTP proxies and firewalls.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	IPHTTPSOut

Core Networking - IPv6 (IPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunneling services.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	41
Local Ports	Any
Remote Ports	Any

Core Networking - Multicast Listener Done (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Multicast Listener Done messages inform local routers that there are no longer any members remaining for a specific multicast address on the subnet.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Query (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	An IPv6 multicast-capable router uses the Multicast Listener Query message to query a link for multicast group membership.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Report (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Report v2 (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Multicast Listener Report v2 message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Neighbor Discovery Advertisement (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Neighbor Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Neighbor Discovery Solicitation (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Neighbor Discovery Solicitations are sent by nodes to discover the link-layer address of another on-link IPv6 node.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Packet Too Big (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Packet Too Big error messages are sent from any node that a packet traverses which is unable to forward the packet because the packet is too large for the next link.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Parameter Problem (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Parameter Problem error messages are sent by nodes as a result of incorrectly generated packets.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Router Advertisement (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Router Advertisement messages are sent by routers to other nodes for stateless auto-configuration.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	fe80::/64
Remote Addresses	LocalSubnet6 ff02::1 fe80::/64

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Router Solicitation (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Router Solicitation messages are sent by nodes seeking routers to provide stateless auto-configuration.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6 ff02::2 fe80::/64

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Teredo (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound UDP rule to allow Teredo edge traversal, a technology that provides address assignment and automatic tunneling for unicast IPv6 traffic when an IPv6/IPv4 host is located behind an IPv4 network address translator.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Core Networking - Time Exceeded (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Time Exceeded error messages are generated from any node that a packet traverses if the Hop Limit value is decremented to zero at any point on the path.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Desktop App Web Viewer

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Desktop App Web Viewer
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Email and accounts

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Email and accounts
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Feedback Hub

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Feedback Hub
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

mDNS (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for mDNS traffic [UDP]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	5353

mDNS (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for mDNS traffic [UDP]
Direction	Outbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	5353

mDNS (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for mDNS traffic [UDP]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	5353

Microsoft Media Foundation Network Source OUT [TCP ALL]

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	OutBound Rule for the Microsoft Media Foundation's Capture SVC to open TCP port to enable RTSP
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	554 8554-8558

Narrator

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Narrator Home
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Start

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Start
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

WFD ASP Coordination Protocol (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for WLAN Service to allow coordination protocol for WFD Service sessions [UDP 7235]
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	UDP
Local Ports	7235
Remote Ports	7235

WFD Driver-only (TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for drivers to communicate over WFD (TCP-Out)
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

WFD Driver-only (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Inbound rule for drivers to communicate over WFD (UDP-Out)
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	System

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Windows Default Lock Screen

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Default Lock Screen
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Defender SmartScreen

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Defender SmartScreen
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Device Management Certificate Installer (TCP out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Allow outbound TCP traffic from Windows Device Management Certificate Installer
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\dmcertinst.exe

Protocols and Ports

Protocol	TCP
Local Ports	49152-65535
Remote Ports	Any

Windows Device Management Device Enroller (TCP out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Allow outbound TCP traffic from Windows Device Management Device Enroller
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\deviceenroller.exe

Protocols and Ports

Protocol	TCP
Local Ports	49152-65535
Remote Ports	80 443

Windows Device Management Enrollment Service (TCP out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Allow outbound TCP traffic from Windows Device Management Enrollment Service
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\svchost.exe

Protocols and Ports

Protocol	TCP
Local Ports	49152-65535
Remote Ports	Any

Windows Device Management Sync Client (TCP out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Allow outbound TCP traffic from Windows Device Management Sync Client
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\omadmclient.exe

Protocols and Ports

Protocol	TCP
Local Ports	49152-65535
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Print

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Print
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Security

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Security
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Shell Experience

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Shell Experience
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Terminal

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Windows Terminal
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Wireless Display (TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for Wireless Display [TCP]
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\WUDFHost.exe

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Wireless Display (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Outbound rule for Wireless Display [UDP]
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	C:\WINDOWS\system32\WUDFHost.exe

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Work or school account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Work or school account
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Your account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Security Type	None
Description	Your account
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Programs And Services

Application	All applications that meet the specified conditions

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Patches

This section provides information about the system-wide updates (commonly referred to as a quick-fix engineering (QFE) updates) installed on this machine.

4 Windows Patches

HotFix ID	Description	Installed By	Installed On
KB5046306	Security Update	NT AUTHORITY\SYSTEM	11/5/2024
KB5049622	Update	NT AUTHORITY\SYSTEM	2/12/2025
KB5051987	Security Update	NT AUTHORITY\SYSTEM	2/12/2025
KB5052085	Security Update	NT AUTHORITY\SYSTEM	2/12/2025

Windows Update Configuration

Windows Update is a service provided by Microsoft that provides updates for the Windows operating system and installed components. It can be expanded to provide support for other Microsoft software and is then referred to as “Microsoft Update”.

The system can be configured either directly or using Group Policy, and updates can be obtained directly from Microsoft over an internet connection or from a Windows Software Update (WSUS) Server installed on the intranet.

General Settings	
Windows Update Mode	Never check for updates (not recommended)
Recommended Updates	Unknown
Include other Microsoft products	False
Registered Services	Windows Update

Advanced	
Allow non-administrators to receive update notifications	Unknown
Automatic Maintenance Enabled	False

Windows Update Server	
Enable Windows Update Server	False

Windows Update History

Windows Update is a service provided by Microsoft that provides updates for the Windows operating system and installed components. This section provides historical information about the updates that have been installed on this machine.

5 History Items

Action Date	Title	Operation	Result
Wednesday, February 12, 2025 5:29:31 PM	2025-01 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Microsoft server operating system version 24H2 for x64 (KB5049622)	Install	Succeeded
Wednesday, February 12, 2025 5:51:19 PM	2025-02 Cumulative Update for Microsoft server operating system version 24H2 for x64-based Systems (KB5051987)	Install	Succeeded
Wednesday, November 27, 2024 1:50:54 PM	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.499.0) - Current Channel (Broad)	Install	Failed
Wednesday, February 12, 2025 5:21:37 PM	Update for Windows Security platform - KB5007651 (Version 10.0.27703.1006)	Install	Succeeded
Wednesday, February 12, 2025 5:21:34 PM	Windows Malicious Software Removal Tool x64 - v5.132 (KB890830)	Install	Succeeded

Software

Provides information about the software and operating system configuration of this machine.

Operating System	
Operating System Name	Microsoft Windows Server 2025 Datacenter
Service Pack	[None Installed]

General	
Installed Programs	15
Event Logs	8
Environment Variables	21
Scheduled Tasks	4

.NET Framework

The .NET Framework is a software framework developed by Microsoft that runs primarily on Microsoft Windows.

Common Language Runtime (CLR) 1

Name	Status	Service Pack
.NET Framework 1.0	Not Installed	
.NET Framework 1.1	Not Installed	

Common Language Runtime (CLR) 2

Name	Status	Service Pack
.NET Framework 2.0.50727	Not Installed	
.NET Framework 3.0	Not Installed	
.NET Framework 3.5	Not Installed	

Common Language Runtime (CLR) 4

Name	Status	Service Pack
.NET Framework 4.0 Client Profile	Installed	
.NET Framework 4.0 Extended	Installed	
.NET Framework 4.5	Installed	
.NET Framework 4.5.1	Installed	
.NET Framework 4.5.2	Installed	
.NET Framework 4.6	Installed	
.NET Framework 4.6.1	Installed	
.NET Framework 4.6.2	Installed	
.NET Framework 4.7	Installed	
.NET Framework 4.7.1	Installed	
.NET Framework 4.7.2	Installed	
.NET Framework 4.8	Installed	

Documented Files

Provides information about the files that have been configured to be documented on the XIA Configuration Client.

1 Files

Display Name	Name	Type	Located
Machine Config (.NET 4)	machine.config	.config	True

Machine Config (.NET 4)

Provides information about the files that have been configured to be documented on the XIA Configuration Client.

File Details

Located	True

General

Full Path	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
File Size	35.14 KB
Creation Date	Saturday, December 7, 2019 9:14:55 AM
Last Accessed	Friday, February 14, 2025 3:11:26 PM
Last Modified	Saturday, December 7, 2019 9:12:43 AM
File Type	.config
Hidden	False
Read Only	False

Advanced

Encrypted	False
Compressed	False

Security

Owner	NT AUTHORITY\SYSTEM

6 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
ALL APPLICATION PACKAGES	True	Allow	Read & execute	This folder or file only
ALL RESTRICTED APPLICATION PACKAGES	True	Allow	Read & execute	This folder or file only
BUILTIN\Administrators	True	Allow	Full control	This folder or file only
BUILTIN\IIS_IUSRS	True	Allow	Read & execute	This folder or file only
BUILTIN\Users	True	Allow	Read & execute	This folder or file only
NT AUTHORITY\SYSTEM	True	Allow	Full control	This folder or file only

0 NTFS Audit Rules

There are no audit rules found.

File Contents

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--
Please refer to machine.config.comments for a description and
the default values of each configuration section.

For a full documentation of the schema please refer to
http://go.microsoft.com/fwlink/?LinkId=42127

To improve performance, machine.config should contain only those
settings that differ from their defaults.
-->
<configuration>
<configSections>
<section name="appSettings" type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" restartOnExternalChanges="false" requirePermission="false" />
</configSections>
</configuration>
```

Event Logs

Event logging provides a standard, centralized way for applications and the operating system to record important software and hardware events.

The event logging service records events from various sources and stores them in a single collection called an event log.

8 Event Logs

Name	Type	Maximum File Size	Retention Policy
Application	Administrative	20,480 KB	Overwrite events as needed
Forwarded Events	Operational	20,480 KB	Overwrite events as needed
Hardware Events	Administrative	20,480 KB	Overwrite events as needed
Key Management Service	Administrative	20,480 KB	Overwrite events as needed
Security	Administrative	20,480 KB	Overwrite events as needed
Setup	Operational	1,028 KB	Overwrite events as needed
System	Administrative	20,480 KB	Overwrite events as needed
Windows PowerShell	Administrative	15,360 KB	Overwrite events as needed

Application

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	Application
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\Application.evtx
Log Type	Administrative
File Size	2.07 MB
Record Count	2,747

File Access

Created	Wednesday, November 6, 2024 12:49:18 AM
Last Accessed	Friday, February 14, 2025 3:15:46 PM
Last Modified	Friday, February 14, 2025 3:15:46 PM

Retention

Maximum File Size	20,480 KB
Retention Policy	Overwrite events as needed

Application

Provides information about the recent events written to this event log.

Most recent 10 entries

Type	Date and Time	Source	Event ID	Task Category	Username
Information	Friday, February 14, 2025 3:15:47 PM	Security-SPP	16389	None	N/A
Information	Friday, February 14, 2025 3:15:47 PM	Security-SPP	16394	None	N/A
Information	Friday, February 14, 2025 3:15:22 PM	SceCli	1704	None	N/A
Information	Friday, February 14, 2025 3:15:19 PM	MsiInstaller	1033	None	CONTOSO\sysadmin
Information	Friday, February 14, 2025 3:15:19 PM	MsiInstaller	11707	None	CONTOSO\sysadmin
Information	Friday, February 14, 2025 3:15:18 PM	MsiInstaller	1042	None	NT AUTHORITY\SYSTEM
Information	Friday, February 14, 2025 3:15:18 PM	RestartManager	10001	None	CONTOSO\sysadmin
Information	Friday, February 14, 2025 3:15:17 PM	RestartManager	10000	None	CONTOSO\sysadmin
Information	Friday, February 14, 2025 3:15:16 PM	MsiInstaller	1040	None	CONTOSO\sysadmin
Information	Friday, February 14, 2025 3:11:25 PM	VSS	8224	None	N/A

2/14/2025 3:15:47 PM

Date and Time	Friday, February 14, 2025 3:15:47 PM
Event ID	16,389
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-SPP
Task Category	None
Username	N/A
Message	Grace timer has expired. Hr = 0xC004D30B

2/14/2025 3:15:47 PM

Date and Time	Friday, February 14, 2025 3:15:47 PM
Event ID	16,394
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-SPP
Task Category	None
Username	N/A
Message	Offline downlevel migration succeeded.

2/14/2025 3:15:22 PM

Date and Time	Friday, February 14, 2025 3:15:22 PM
Event ID	1,704
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	SceCli
Task Category	None
Username	N/A
Message	Security policy in the Group policy objects has been applied successfully.

2/14/2025 3:15:19 PM

Date and Time	Friday, February 14, 2025 3:15:19 PM
Event ID	1,033
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	MsiInstaller
Task Category	None
Username	CONTOSO\sysadmin
Message	Windows Installer installed the product. Product Name: Local Administrator Password Solution. Product Version: 6.2.0.0. Product Language: 1033. Manufacturer: Microsoft Corporation. Installation success or error status: 0.

2/14/2025 3:15:19 PM

Date and Time	Friday, February 14, 2025 3:15:19 PM
Event ID	11,707
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	MsiInstaller
Task Category	None
Username	CONTOSO\sysadmin
Message	Product: Local Administrator Password Solution -- Installation completed successfully.

2/14/2025 3:15:18 PM

Date and Time	Friday, February 14, 2025 3:15:18 PM
Event ID	1,042
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	MsiInstaller
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Ending a Windows Installer transaction: C:\Users\sysadmin\Documents\LAPS.x64.msi. Client Process Id: 5304.

2/14/2025 3:15:18 PM

Date and Time	Friday, February 14, 2025 3:15:18 PM
Event ID	10,001
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	RestartManager
Task Category	None
Username	CONTOSO\sysadmin
Message	Ending session 0 started 2025 - 02 - 14T15:15:17.970394600Z.

2/14/2025 3:15:17 PM

Date and Time	Friday, February 14, 2025 3:15:17 PM
Event ID	10,000
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	RestartManager
Task Category	None
Username	CONTOSO\sysadmin
Message	Starting session 0 - 2025 - 02 - 14T15:15:17.970394600Z.

2/14/2025 3:15:16 PM

Date and Time	Friday, February 14, 2025 3:15:16 PM
Event ID	1,040
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	MsiInstaller
Task Category	None
Username	CONTOSO\sysadmin
Message	Beginning a Windows Installer transaction: C:\Users\sysadmin\Documents\LAPS.x64.msi. Client Process Id: 5304.

2/14/2025 3:11:25 PM

Date and Time	Friday, February 14, 2025 3:11:25 PM
Event ID	8,224
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	VSS
Task Category	None
Username	N/A
Message	The VSS service is shutting down due to idle timeout.

Forwarded Events

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	ForwardedEvents
Enabled	False
Classic Log	False
Log Path	%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx
Log Type	Operational
File Size	0 bytes
Record Count	0

File Access

Created	[Not Configured]
Last Accessed	[Not Configured]
Last Modified	[Not Configured]

Retention

Maximum File Size	20,480 KB
Retention Policy	Overwrite events as needed

Forwarded Events

Provides information about the recent events written to this event log.

Most recent 0 entries

There are no event log entries found.

Hardware Events

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	HardwareEvents
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\HardwareEvents.evtx
Log Type	Administrative
File Size	68 KB
Record Count	0

File Access

Created	Wednesday, November 6, 2024 12:49:18 AM
Last Accessed	Wednesday, November 6, 2024 12:50:12 AM
Last Modified	Wednesday, November 6, 2024 12:50:12 AM

Retention

Maximum File Size	20,480 KB
Retention Policy	Overwrite events as needed

Hardware Events

Provides information about the recent events written to this event log.

Most recent 0 entries

There are no event log entries found.

Key Management Service

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings	
Name	Key Management Service
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\Key Management Service.evtx
Log Type	Administrative
File Size	68 KB
Record Count	0

File Access	
Created	Wednesday, November 6, 2024 12:49:18 AM
Last Accessed	Wednesday, November 6, 2024 12:50:12 AM
Last Modified	Wednesday, November 6, 2024 12:50:12 AM

Retention	
Maximum File Size	20,480 KB
Retention Policy	Overwrite events as needed

Key Management Service

Provides information about the recent events written to this event log.

Most recent 0 entries

There are no event log entries found.

Security

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	Security
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\Security.evtx
Log Type	Administrative
File Size	20 MB
Record Count	22,379

File Access

Created	Wednesday, November 6, 2024 12:49:18 AM
Last Accessed	Friday, February 14, 2025 3:15:39 PM
Last Modified	Friday, February 14, 2025 3:15:39 PM

Retention

Maximum File Size	20,480 KB
Retention Policy	Overwrite events as needed

Security

Provides information about the recent events written to this event log.

Most recent 10 entries

Type	Date and Time	Source	Event ID	Task Category	Username
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4634	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4624	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4672	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4648	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4672	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4624	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4672	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4624	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4672	Logoff	N/A
Success Audit	Friday, February 14, 2025 3:15:23 PM	Security-Auditing	4624	Logoff	N/A

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,634
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	An account was logged off. Subject: Security ID: S-1-5-18 Account Name: XCS-2K25-DEMO$ Account Domain: CONTOSO Logon ID: 0x2F88A26 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,624
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: XCS-2K25-DEMO$ Account Domain: CONTOSO.COM Logon ID: 0x2F88A26 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {bedb89fc-c46a-e1aa-dfa5-af2430f746ee} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,672
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: XCS-2K25-DEMO$ Account Domain: CONTOSO Logon ID: 0x2F88A26 Privileges: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,648
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: XCS-2K25-DEMO$ Account Domain: CONTOSO Logon ID: 0x3E7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: XCS-2K25-DEMO$ Account Domain: CONTOSO.COM Logon GUID: {bedb89fc-c46a-e1aa-dfa5-af2430f746ee} Target Server: Target Server Name: xcs-2k25-demo$ Additional Information: xcs-2k25-demo$ Process Information: Process ID: 0x1894 Process Name: C:\Windows\System32\taskhostw.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account’s credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,672
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,624
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: XCS-2K25-DEMO$ Account Domain: CONTOSO Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,672
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,624
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: XCS-2K25-DEMO$ Account Domain: CONTOSO Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,672
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	4,624
Entry Type	Success Audit
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Security-Auditing
Task Category	Logoff
Username	N/A
Message	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: XCS-2K25-DEMO$ Account Domain: CONTOSO Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Setup

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	Setup
Enabled	True
Classic Log	False
Log Path	%SystemRoot%\System32\Winevt\Logs\Setup.evtx
Log Type	Operational
File Size	1 MB
Record Count	435

File Access

Created	Wednesday, November 6, 2024 12:49:18 AM
Last Accessed	Wednesday, February 12, 2025 6:08:06 PM
Last Modified	Wednesday, February 12, 2025 6:08:06 PM

Retention

Maximum File Size	1,028 KB
Retention Policy	Overwrite events as needed

Setup

Provides information about the recent events written to this event log.

Most recent 10 entries

Type	Date and Time	Source	Event ID	Task Category	Username
Information	Wednesday, February 12, 2025 6:06:46 PM	Servicing	2	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 6:06:45 PM	Servicing	2	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 6:04:39 PM	Servicing	4	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 5:51:16 PM	Servicing	4	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 5:48:00 PM	Servicing	1	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 5:47:54 PM	Servicing	2	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 5:44:59 PM	Servicing	1	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 5:44:40 PM	Servicing	2	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 5:44:34 PM	Servicing	1	None	NT AUTHORITY\SYSTEM
Information	Wednesday, February 12, 2025 5:31:00 PM	Servicing	2	None	NT AUTHORITY\SYSTEM

2/12/2025 6:06:46 PM

Date and Time	Wednesday, February 12, 2025 6:06:46 PM
Event ID	2
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Package KB5051987 was successfully changed to the Installed state.

2/12/2025 6:06:45 PM

Date and Time	Wednesday, February 12, 2025 6:06:45 PM
Event ID	2
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Package KB5049622 was successfully changed to the Installed state.

2/12/2025 6:04:39 PM

Date and Time	Wednesday, February 12, 2025 6:04:39 PM
Event ID	4
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	A reboot is necessary before package KB5049622 can be changed to the Installed state.

2/12/2025 5:51:16 PM

Date and Time	Wednesday, February 12, 2025 5:51:16 PM
Event ID	4
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	A reboot is necessary before package KB5051987 can be changed to the Installed state.

2/12/2025 5:48:00 PM

Date and Time	Wednesday, February 12, 2025 5:48:00 PM
Event ID	1
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Initiating changes for package KB5051987. Current state is Staged. Target state is Installed. Client id: UpdateAgentLCU.

2/12/2025 5:47:54 PM

Date and Time	Wednesday, February 12, 2025 5:47:54 PM
Event ID	2
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Package KB5051987 was successfully changed to the Staged state.

2/12/2025 5:44:59 PM

Date and Time	Wednesday, February 12, 2025 5:44:59 PM
Event ID	1
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Initiating changes for package KB5051987. Current state is Absent. Target state is Staged. Client id: UpdateAgentLCU.

2/12/2025 5:44:40 PM

Date and Time	Wednesday, February 12, 2025 5:44:40 PM
Event ID	2
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Package KB5052085 was successfully changed to the Installed state.

2/12/2025 5:44:34 PM

Date and Time	Wednesday, February 12, 2025 5:44:34 PM
Event ID	1
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Initiating changes for package KB5052085. Current state is Staged. Target state is Installed. Client id: UpdateAgentLCU.

2/12/2025 5:31:00 PM

Date and Time	Wednesday, February 12, 2025 5:31:00 PM
Event ID	2
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Package KB5052085 was successfully changed to the Staged state.

System

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	System
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\System.evtx
Log Type	Administrative
File Size	3.07 MB
Record Count	6,336

File Access

Created	Wednesday, November 6, 2024 12:49:18 AM
Last Accessed	Friday, February 14, 2025 3:15:39 PM
Last Modified	Friday, February 14, 2025 3:15:39 PM

Retention

Maximum File Size	20,480 KB
Retention Policy	Overwrite events as needed

System

Provides information about the recent events written to this event log.

Most recent 10 entries

Type	Date and Time	Source	Event ID	Task Category	Username
Information	Friday, February 14, 2025 3:15:47 PM	Service Control Manager	7036	None	N/A
Information	Friday, February 14, 2025 3:15:23 PM	Service Control Manager	7036	None	N/A
Information	Friday, February 14, 2025 3:15:23 PM	Service Control Manager	7036	None	N/A
Information	Friday, February 14, 2025 3:15:23 PM	Service Control Manager	7036	None	N/A
Information	Friday, February 14, 2025 3:15:23 PM	Service Control Manager	7036	None	N/A
Information	Friday, February 14, 2025 3:15:23 PM	Service Control Manager	7036	None	N/A
Information	Friday, February 14, 2025 3:15:23 PM	GroupPolicy	1502	None	NT AUTHORITY\SYSTEM
Information	Friday, February 14, 2025 3:15:21 PM	FilterManager	1	None	NT AUTHORITY\SYSTEM
Information	Friday, February 14, 2025 3:15:08 PM	Service Control Manager	7036	None	N/A
Information	Friday, February 14, 2025 3:15:08 PM	FilterManager	6	None	NT AUTHORITY\SYSTEM

2/14/2025 3:15:47 PM

Date and Time	Friday, February 14, 2025 3:15:47 PM
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Software Protection service entered the running state.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Delivery Optimization service entered the stopped state.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Delivery Optimization service entered the running state.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The WaaSMedicSvc service entered the running state.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Portable Device Enumerator Service service entered the running state.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Network Connectivity Assistant service entered the stopped state.

2/14/2025 3:15:23 PM

Date and Time	Friday, February 14, 2025 3:15:23 PM
Event ID	1,502
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	GroupPolicy
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	The Group Policy settings for the computer were processed successfully. New settings from 2 Group Policy objects were detected and applied.

2/14/2025 3:15:21 PM

Date and Time	Friday, February 14, 2025 3:15:21 PM
Event ID	1
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	FilterManager
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	File System Filter 'FileInfo' (Version 10.0, 2093 - 04 - 02T01:29:43.000000000Z) unloaded successfully.

2/14/2025 3:15:08 PM

Date and Time	Friday, February 14, 2025 3:15:08 PM
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Diagnostic System Host service entered the running state.

2/14/2025 3:15:08 PM

Date and Time	Friday, February 14, 2025 3:15:08 PM
Event ID	6
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	FilterManager
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	File System Filter 'FileInfo' (10.0, 2093 - 04 - 02T01:29:43.000000000Z) has successfully loaded and registered with Filter Manager.

Windows PowerShell

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	Windows PowerShell
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\Windows PowerShell.evtx
Log Type	Administrative
File Size	3.07 MB
Record Count	839

File Access

Created	Wednesday, November 6, 2024 12:49:18 AM
Last Accessed	Friday, February 14, 2025 3:09:51 PM
Last Modified	Friday, February 14, 2025 3:09:51 PM

Retention

Maximum File Size	15,360 KB
Retention Policy	Overwrite events as needed

Windows PowerShell

Provides information about the recent events written to this event log.

Most recent 10 entries

Type	Date and Time	Source	Event ID	Task Category	Username
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	800	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	400	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	600	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	600	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	600	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	600	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	600	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	600	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	600	Pipeline Execution Details	N/A
Information	Friday, February 14, 2025 3:15:43 PM	PowerShell	600	Pipeline Execution Details	N/A

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	800
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Pipeline execution details for command line: else { $result = Add-Type -TypeDefinition $securitySupportCoreSource } . Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=213 UserId=CONTOSO\sysadmin HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion=5.1.26100.2161 RunspaceId=f8e5786b-84b1-4c96-80f6-0d787d61cd8a PipelineId=4 ScriptName= CommandLine=else { $result = Add-Type -TypeDefinition $securitySupportCoreSource } Details: CommandInvocation(Add-Type): "Add-Type" ParameterBinding(Add-Type): name="TypeDefinition"; value="using System; using System.Runtime.InteropServices; using System.Security.Principal; using System.Text; namespace CENTREL.XIA.Network.Management.Windows.SecuritySupportCore { /// <summary> /// Provides security support functions. /// </summary> public class SecuritySupportCore { /// <summary> /// The LookupAccountName function accepts the name of a system and an account as input. It retrieves a security identifier (SID) for the account and the name of the domain on which the account was found. /// </summary> /// <param name="systemName">The name of the system on which to execute the method.</param> /// <param name="accountName">The account name for which the SID should be obtained in the format "domain\username".</param> /// <param name="sid">A pointer to a buffer that receives the SID structure.</param> /// <param name="cbSid">A pointer to a variable. On input, this value specifies the size, in bytes, of the Sid buffer.</param> /// <param name="referencedDomainName">A pointer to a buffer that receives the name of the domain where the account name is found.</param> /// <param name="cbReferencedDomainName">A pointer to a variable. On input, this value specifies the size, in TCHARs, of the ReferencedDomainName buffer. </param> /// <param name="use">A pointer to a SID_NAME_USE enumerated type that indicates the type of the account when the function returns.</param> /// <returns>A System.Boolean value that indicates whether the method succeeded.</returns> /// <remarks>http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159(v=vs.8 5).aspx</remarks> [DllImport("advapi32.dll", CharSet = CharSet.Auto, SetLastError = true)] internal static extern bool LookupAccountName([In, MarshalAs(UnmanagedType.LPTStr)] string systemName, [In, MarshalAs(UnmanagedType.LPTStr)] string accountName, IntPtr sid, ref int cbSid, StringBuilder referencedDomainName, ref int cbReferencedDomainName,

```
            out int use
        );


        /// <summary>
        /// Obtains the security identifier of the account name on the specified remote machine.
        /// </summary>
        /// <param name="machineName">The name of the remote system on which to perform the
resolution.</param>
        /// <param name="accountName">The name of the account to resolve in the format
"domain\username".</param>
        /// <returns>The security identifier on the remote machine in SDDL format.</returns>
        public static String GetAccountSid(String machineName, String accountName)
        {
            IntPtr sidPtr = IntPtr.Zero;
            try
            {
                int ERROR_INSUFFICIENT_BUFFER = 122;
                int ERROR_INVALID_FLAGS = 1004;
                int sidLength = 0;
                int domainLength = 0;
                int use = 0;
                StringBuilder domainName = new StringBuilder();
                int errorCode = 0;
                LookupAccountName(machineName, accountName, sidPtr, ref sidLength, domainName, ref
domainLength, out use);
                errorCode = Marshal.GetLastWin32Error();
                if (errorCode != ERROR_INSUFFICIENT_BUFFER && errorCode != ERROR_INVALID_FLAGS) { throw
 new InvalidOperationException(String.Format("Error code {0}", errorCode)); }
                domainName = new StringBuilder(domainLength);
                sidPtr = Marshal.AllocHGlobal(sidLength);
                bool success = LookupAccountName(machineName, accountName, sidPtr, ref sidLength,
domainName, ref domainLength, out use);
                if (success)
                {
                    SecurityIdentifier sid = new SecurityIdentifier(sidPtr);
                    return sid.ToString();
                }
                errorCode = Marshal.GetLastWin32Error();
                throw new InvalidOperationException(String.Format("Error code {0}", errorCode));
            }
            catch (Exception ex) { throw new ArgumentException(String.Format("Could not get the SID for the account
 name '{0}' on machine '{1}'. {2}", accountName, machineName, ex.Message), ex); }
            finally { Marshal.FreeHGlobal(sidPtr); }
        }

    }
}
"
```

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	400
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Engine state is changed from None to Available. Details: NewEngineState=Available PreviousEngineState=None SequenceNumber=211 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion=5.1.26100.2161 RunspaceId=f8e5786b-84b1-4c96-80f6-0d787d61cd8a PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	600
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Provider "WSMan" is Started. Details: ProviderName=WSMan NewProviderState=Started SequenceNumber=209 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	600
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Provider "Certificate" is Started. Details: ProviderName=Certificate NewProviderState=Started SequenceNumber=207 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	600
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Provider "Variable" is Started. Details: ProviderName=Variable NewProviderState=Started SequenceNumber=205 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	600
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started SequenceNumber=203 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	600
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Provider "FileSystem" is Started. Details: ProviderName=FileSystem NewProviderState=Started SequenceNumber=201 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	600
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Provider "Environment" is Started. Details: ProviderName=Environment NewProviderState=Started SequenceNumber=199 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	600
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Provider "Alias" is Started. Details: ProviderName=Alias NewProviderState=Started SequenceNumber=197 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

2/14/2025 3:15:43 PM

Date and Time	Friday, February 14, 2025 3:15:43 PM
Event ID	600
Entry Type	Information
Machine Name	XCS-2K25-DEMO.contoso.com
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	Provider "Registry" is Started. Details: ProviderName=Registry NewProviderState=Started SequenceNumber=195 HostName=Default Host HostVersion=5.1.26100.2161 HostId=af0e2317-39d0-428d-bcf7-fc857b822cd2 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

Environment Variables

Details the environmental variables found on this machine. Environmental variables can be accessed on Windows Machines by using the SET command at a command prompt. Variables can be user based or SYSTEM variables which are accessible to all users.

21 Environment Variables

Variable Name	Username	Value
%ALLUSERSPROFILE%	<SYSTEM>	C:\ProgramData
%CommonProgramFiles%	<SYSTEM>	C:\Program Files\Common Files
%ComSpec%	<SYSTEM>	C:\WINDOWS\system32\cmd.exe
%DriverData%	<SYSTEM>	C:\Windows\System32\Drivers\DriverData
%NUMBER_OF_PROCESSORS%	<SYSTEM>	1
%OS%	<SYSTEM>	Windows_NT
%Path%	<SYSTEM>	C:\WINDOWS\system32 C:\WINDOWS C:\WINDOWS\System32\Wbem C:\WINDOWS\System32\WindowsPowerShell\v1.0\ C:\WINDOWS\System32\OpenSSH\ C:\Program Files (x86)\Microsoft SQL Server\160\Tools\Binn\ C:\Program Files\Microsoft SQL Server\160\Tools\Binn\ C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\ C:\Program Files\Microsoft SQL Server\160\DTS\Binn\
%PATHEXT%	<SYSTEM>	.COM .EXE .BAT .CMD .VBS .VBE .JS .JSE .WSF .WSH .MSC
%PROCESSOR_ARCHITECTURE%	<SYSTEM>	AMD64
%PROCESSOR_IDENTIFIER%	<SYSTEM>	Intel64 Family 6 Model 165 Stepping 2, GenuineIntel

%PROCESSOR_LEVEL%	<SYSTEM>	6
%PROCESSOR_REVISION%	<SYSTEM>	a502
%ProgramFiles%	<SYSTEM>	C:\Program Files
%ProgramFiles(x86)%	<SYSTEM>	C:\Program Files (x86)
%PSModulePath%	<SYSTEM>	C:\Program Files\WindowsPowerShell\Modules C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules C:\Program Files (x86)\Microsoft SQL Server\160\Tools\PowerShell\Modules\
%SystemDrive%	<SYSTEM>	C:
%SystemRoot%	<SYSTEM>	C:\WINDOWS
%TEMP%	<SYSTEM>	C:\WINDOWS\TEMP
%TMP%	<SYSTEM>	C:\WINDOWS\TEMP
%USERNAME%	<SYSTEM>	SYSTEM
%windir%	<SYSTEM>	C:\WINDOWS

Installed Software

Provides information about the programs installed on this Windows machine.

15 Installed Programs

Name	Publisher	Platform	Version	Installation Date
Browser for SQL Server 2022	Microsoft Corporation	32 bit	16.0.1000.6	Wednesday, November 27, 2024
Google Chrome	Google LLC	32 bit	132.0.6834.197	Thursday, February 13, 2025
Local Administrator Password Solution	Microsoft Corporation	64 bit	6.2.0.0	Friday, February 14, 2025
Microsoft Edge	Microsoft Corporation	32 bit	133.0.3065.59	Wednesday, February 12, 2025
Microsoft Edge WebView2 Runtime	Microsoft Corporation	32 bit	133.0.3065.59	Tuesday, February 11, 2025
Microsoft ODBC Driver 17 for SQL Server	Microsoft Corporation	64 bit	17.4.1.1	Wednesday, November 27, 2024
Microsoft ODBC Driver 18 for SQL Server	Microsoft Corporation	64 bit	18.1.2.1	Friday, January 3, 2025
Microsoft OLE DB Driver for SQL Server	Microsoft Corporation	64 bit	18.2.4.0	Wednesday, November 27, 2024
Microsoft SQL Server 2022 (64-bit)	Microsoft Corporation	64 bit		Wednesday, November 27, 2024
Microsoft SQL Server 2022 Setup (English)	Microsoft Corporation	64 bit	16.0.1000.6	Wednesday, November 27, 2024
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532	Microsoft Corporation	32 bit	14.36.32532.0	Tuesday, November 26, 2024
Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532	Microsoft Corporation	32 bit	14.36.32532.0	Tuesday, November 26, 2024
Microsoft VSS Writer for SQL Server 2022	Microsoft Corporation	64 bit	16.0.1000.6	Wednesday, November 27, 2024
VMware Tools	VMware, Inc.	64 bit	12.4.5.23787635	Tuesday, November 5, 2024
XIA Configuration Server	CENTREL Solutions	64 bit	17.0.5	Friday, February 7, 2025

Internet Settings

This section provides information about the Internet Settings for the machine including the system level proxy settings.

Internet Settings	
Internet Explorer Version	11.1882.26100.0

System Proxy	
Connection Type	Direct Connection

Internet Explorer Enhanced Security	
Administrators	True
Users	True

ODBC Configuration

Open Database Connectivity (ODBC) is a standard interface for accessing data in an array of relational and non-relational database management systems (DBMS) without the need for independent software vendors and corporate developers to learn multiple application programming interfaces.

Drivers	23
Data Sources	0

ODBC Drivers

An ODBC driver provides the ability to translate commands between an ODBC client applications and the backend data source.

23 ODBC Drivers

Name	Platform	ODBC Version	File Version	Filename
Driver da Microsoft para arquivos texto (*.txt; *.csv)	x86	2.50		odbcjt32.dll
Driver do Microsoft Access (*.mdb)	x86	2.50		odbcjt32.dll
Driver do Microsoft dBase (*.dbf)	x86	2.50		odbcjt32.dll
Driver do Microsoft Excel(*.xls)	x86	2.50		odbcjt32.dll
Driver do Microsoft Paradox (*.db)	x86	2.50		odbcjt32.dll
Microsoft Access Driver (*.mdb)	x86	2.50		odbcjt32.dll
Microsoft Access-Treiber (*.mdb)	x86	2.50		odbcjt32.dll
Microsoft dBase Driver (*.dbf)	x86	2.50		odbcjt32.dll
Microsoft dBase-Treiber (*.dbf)	x86	2.50		odbcjt32.dll
Microsoft Excel Driver (*.xls)	x86	2.50		odbcjt32.dll
Microsoft Excel-Treiber (*.xls)	x86	2.50		odbcjt32.dll
Microsoft ODBC for Oracle	x86	2.50		msorcl32.dll
Microsoft Paradox Driver (*.db)	x86	2.50		odbcjt32.dll
Microsoft Paradox-Treiber (*.db)	x86	2.50		odbcjt32.dll
Microsoft Text Driver (*.txt; *.csv)	x86	2.50		odbcjt32.dll
Microsoft Text-Treiber (*.txt; *.csv)	x86	2.50		odbcjt32.dll
ODBC Driver 17 for SQL Server	x86	3.80	2017.174.1.1	msodbcsql17.dll
ODBC Driver 17 for SQL Server	x64	3.80	2017.174.1.1	msodbcsql17.dll
ODBC Driver 18 for SQL Server	x86	3.80	2018.181.2.1	msodbcsql18.dll
ODBC Driver 18 for SQL Server	x64	3.80	2018.181.2.1	msodbcsql18.dll
SQL Server	x86	3.50	6.2.26100.3037	SQLSRV32.dll
SQL Server	x64	3.50	6.2.26100.3037	SQLSRV32.dll
SQL Server Native Client RDA 11.0	x64	3.80	2011.110.5069.66	sqlnclirda11.dll

Data Sources

A data source, also known as a data source name (DSN) provides the information required to connect to an ODBC compliant data source such as a Microsoft SQL server or Excel Spreadsheet. This information includes the ODBC driver to use, the location of the database file or server and other settings such as the connection credentials.

There are no ODBC system data sources found on this machine.

Operating System

Provides details about the general operating system configuration.

Operating System

Operating System Name	Microsoft Windows Server 2025 Datacenter
Service Pack	[None Installed]

License and Activation

Display Name	Windows(R), ServerDatacenter edition
License State	Licensed
Partial Product Key	XXXXX-XXXXX-XXXXX-XXXXX-PG4G6
Product Key Channel	Volume:MAK

General

Version	10.0.26100
Operating System Architecture	64-bit
Server Installation Type	Full Server
Build Number	26100
Build Type	Multiprocessor Free
Code Page	1252
Country Code	44
Last BootUp Time	Wednesday, February 12, 2025 6:05:28 PM
Install Date	Tuesday, November 26, 2024 2:22:50 PM
Locale	0809
MUI Languages	en-US
Operating System Language	1033
Serial Number	00491-60000-07877-AA615
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32

Naming and Role

Domain	contoso.com
Domain Role	Member Server
NetBIOS Name	XCS-2K25-DEMO
Fully Qualified Domain Name	xcs-2k25-demo.contoso.com

Timezone

Time Zone Name	(UTC+00:00) Dublin, Edinburgh, Lisbon, London
Daylight In Effect	False
Time Zone Bias	0

Registry

Registry Size (Current)	128
Registry Size (Maximum)	4,095

Page Files

Automatically manage paging file size for all drives

PowerShell Settings

Windows PowerShell is a task-based command-line shell and scripting language built on the .NET Framework designed specifically for system administration.

PowerShell Settings

Is Installed	True
Version	Version 5.1.26100.2161
Runtime Version	4.0.30319.42000
Compatible Versions	1.0 2.0 3.0 4.0 5.0 5.1.26100.2161
Machine Execution Policy	Remote Signed
Machine Execution Policy Source	Local

Permissions

Type	Principal	Access
Allow	BUILTIN\Administrators	Full Control (All Operations)
Allow	NT AUTHORITY\INTERACTIVE	Full Control (All Operations)
Allow	BUILTIN\Remote Management Users	Full Control (All Operations)

Audit Rules

Type	Principal	Access
Failure	Everyone	Full Control (All Operations)
Succes s	Everyone	Execute (Invoke), Write (Put, Delete, Create)

Processes

Provides information about the processes that were running at the time of the scan.

145 Processes

Image Name	PID	CPU %	Memory (KB)	Description
AggregatorHost.exe	2808	0	896	Microsoft (R) Aggregator Host
ApplicationFrameHost.exe	5780	0	3,732	Application Frame Host
audiodg.exe	8648	0	3,896	Windows Audio Device Graph Isolation
CENTREL.XIA.Configuration.Agents.TestHarness.exe	3356	0	50,060	CENTREL.XIA.Configuration.Agents.TestHarness
CENTREL.XIA.Configuration.Client.AdministrationTools.exe	8532	5	52,148	XIA Configuration Client Administration Tool
CENTREL.XIA.Configuration.Server.Scheduler.exe	3748	0	15,700	CENTREL.XIA.Configuration.Server.Scheduler
CENTREL.XIA.Configuration.Service.exe	2520	0	393,340	XIA Configuration Service
chrome.exe	6388	0	860	Google Chrome
chrome.exe	6696	0	109,788	Google Chrome
chrome.exe	6688	0	6,848	Google Chrome
chrome.exe	6624	0	1,996	Google Chrome
chrome.exe	6572	0	7,272	Google Chrome
chrome.exe	6560	0	5,320	Google Chrome
chrome.exe	6172	0	2,960	Google Chrome
chrome.exe	6372	0	55,528	Google Chrome
conhost.exe	8644	0	2,004	Console Window Host
csrss.exe	484	0	852	
csrss.exe	584	0	1,036	
ctfmon.exe	5600	0	4,124	CTF Loader
DataExchangeHost.exe	2088	0	5,680	Data Exchange Host

dllhost.exe	1340	0	1,496	COM Surrogate
dllhost.exe	3844	0	1,800	COM Surrogate
dllhost.exe	5208	0	2,220	COM Surrogate
dwm.exe	260	5	103,264	Desktop Window Manager
explorer.exe	2544	0	138,480	Windows Explorer
explorer.exe	8292	0	11,196	Windows Explorer
fontdrvhost.exe	796	0	2,596	Usermode Font Driver Host
fontdrvhost.exe	788	0	500	Usermode Font Driver Host
lsass.exe	704	0	5,696	Local Security Authority Process
mmc.exe	1748	5	6,564	Microsoft Management Console
MoUsoCoreWorker.exe	4300	0	8,736	MoUSO Core Worker Process
msdtc.exe	4148	0	904	Microsoft Distributed Transaction Coordinator Service
msiexec.exe	3076	0	3,156	Windows® installer
notepad.exe	4420	0	3,212	Notepad
notepad.exe	3020	0	3,812	Notepad
powershell.exe	7756	0	30,124	Windows PowerShell
procexp64.exe	4864	0	4,712	Sysinternals Process Explorer
Registry	76	0	5,068	
RuntimeBroker.exe	5468	0	3,688	Runtime Broker
RuntimeBroker.exe	2220	0	1,432	Runtime Broker
RuntimeBroker.exe	7500	0	2,496	Runtime Broker
RuntimeBroker.exe	5436	0	7,448	Runtime Broker
SearchHost.exe	5288	0	132	
SecurityHealthService.exe	6828	0	2,812	
services.exe	680	0	6,076	
ShellExperienceHost.exe	216	0	60	Windows Shell Experience Host

ShellHost.exe	2932	0	2,228	ShellHost
sihost.exe	2012	0	3,996	Shell Infrastructure Host
smartscreen.exe	6640	0	1,512	Windows Defender SmartScreen
smss.exe	324	0	132	
spoolsv.exe	2348	0	2,832	Spooler SubSystem App
sppsvc.exe	9440	0	3,660	
sqlceip.exe	644	0	43,608	Sql Server Telemetry Client
sqlservr.exe	2052	0	285,628	SQL Server Windows NT - 64 Bit
sqlwriter.exe	2872	0	760	SQL Server VSS Writer - 64 Bit
StartMenuExperienceHost.exe	5276	0	31,012	Windows Start Experience Host
svchost.exe	2788	0	3,320	Host Process for Windows Services
svchost.exe	2236	0	13,204	Host Process for Windows Services
svchost.exe	4356	0	2,048	Host Process for Windows Services
svchost.exe	3064	0	2,020	Host Process for Windows Services
svchost.exe	2056	0	716	Host Process for Windows Services
svchost.exe	2184	0	1,204	Host Process for Windows Services
svchost.exe	2212	0	5,768	Host Process for Windows Services
svchost.exe	2568	0	1,184	Host Process for Windows Services
svchost.exe	2248	0	1,456	Host Process for Windows Services
svchost.exe	2404	0	984	Host Process for Windows Services
svchost.exe	2496	0	1,460	Host Process for Windows Services
svchost.exe	1928	0	4,516	Host Process for Windows Services
svchost.exe	2584	0	512	Host Process for Windows Services
svchost.exe	2600	0	2,324	Host Process for Windows Services
svchost.exe	2240	0	1,000	Host Process for Windows Services
svchost.exe	2608	0	2,348	Host Process for Windows Services

svchost.exe	3788	0	8,192	Host Process for Windows Services
svchost.exe	4240	0	2,104	Host Process for Windows Services
svchost.exe	4116	0	2,452	Host Process for Windows Services
svchost.exe	2736	0	1,308	Host Process for Windows Services
svchost.exe	6272	0	1,052	Host Process for Windows Services
svchost.exe	1852	0	1,040	Host Process for Windows Services
svchost.exe	1836	0	980	Host Process for Windows Services
svchost.exe	4848	0	908	Host Process for Windows Services
svchost.exe	1684	0	584	Host Process for Windows Services
svchost.exe	1652	0	1,956	Host Process for Windows Services
svchost.exe	4528	0	1,664	Host Process for Windows Services
svchost.exe	4792	0	756	Host Process for Windows Services
svchost.exe	3184	0	1,520	Host Process for Windows Services
svchost.exe	2460	0	2,036	Host Process for Windows Services
svchost.exe	2620	0	19,484	Host Process for Windows Services
svchost.exe	3672	0	708	Host Process for Windows Services
svchost.exe	1104	0	2,064	Host Process for Windows Services
svchost.exe	1624	0	8,016	Host Process for Windows Services
svchost.exe	2864	0	704	Host Process for Windows Services
svchost.exe	4248	0	1,224	Host Process for Windows Services
svchost.exe	2976	0	464	Host Process for Windows Services
svchost.exe	972	0	1,508	Host Process for Windows Services
svchost.exe	900	0	5,452	Host Process for Windows Services
svchost.exe	856	0	5,456	Host Process for Windows Services
svchost.exe	1092	0	1,268	Host Process for Windows Services
svchost.exe	3668	0	3,988	Host Process for Windows Services

svchost.exe	2880	0	1,036	Host Process for Windows Services
svchost.exe	896	0	2,920	Host Process for Windows Services
svchost.exe	5520	0	1,300	Host Process for Windows Services
svchost.exe	784	0	1,324	Host Process for Windows Services
svchost.exe	1312	0	1,312	Host Process for Windows Services
svchost.exe	1348	0	3,144	Host Process for Windows Services
svchost.exe	1528	0	14,208	Host Process for Windows Services
svchost.exe	1576	0	3,984	Host Process for Windows Services
svchost.exe	1252	0	976	Host Process for Windows Services
svchost.exe	1288	0	748	Host Process for Windows Services
svchost.exe	1028	0	928	Host Process for Windows Services
svchost.exe	1304	0	1,644	Host Process for Windows Services
svchost.exe	8416	0	1,252	Host Process for Windows Services
svchost.exe	1920	0	784	Host Process for Windows Services
svchost.exe	6200	0	3,828	Host Process for Windows Services
svchost.exe	4780	0	3,160	Host Process for Windows Services
svchost.exe	1592	0	1,360	Host Process for Windows Services
svchost.exe	5444	0	2,540	Host Process for Windows Services
svchost.exe	5504	0	4,064	Host Process for Windows Services
svchost.exe	7264	0	1,272	Host Process for Windows Services
svchost.exe	1152	0	1,360	Host Process for Windows Services
svchost.exe	1068	0	996	Host Process for Windows Services
svchost.exe	3660	0	1,680	Host Process for Windows Services
svchost.exe	4124	0	3,340	Host Process for Windows Services
svchost.exe	5916	0	1,372	Host Process for Windows Services
svchost.exe	1052	0	1,160	Host Process for Windows Services

svchost.exe	1168	0	2,312	Host Process for Windows Services
svchost.exe	6344	0	1,680	Host Process for Windows Services
svchost.exe	7068	0	1,416	
System	4	0	12	
System Idle Process	0	53	8	
taskhostw.exe	4596	0	2,040	Host Process for Windows Tasks
taskhostw.exe	6292	0	0	Host Process for Windows Tasks
taskhostw.exe	8496	0	2,352	Host Process for Windows Tasks
UserOOBEBroker.exe	7088	0	844	User OOBE Broker
VGAuthService.exe	3012	0	888	VMware Guest Authentication Service
vm3dservice.exe	3360	0	704	VMware SVGA Helper Service
vm3dservice.exe	3004	0	636	VMware SVGA Helper Service
vmtoolsd.exe	1272	0	24,244	VMware Tools Core Service
vmtoolsd.exe	3028	0	4,600	VMware Tools Core Service
w3wp.exe	3740	0	446,060	IIS Worker Process
wininit.exe	576	0	616	
winlogon.exe	632	0	1,176	Windows Logon Application
WmiApSrv.exe	10152	0	1,408	WMI Performance Reverse Adapter
WmiPrvSE.exe	4084	0	15,272	WMI Provider Host
WmiPrvSE.exe	1440	0	35,948	WMI Provider Host
WmiPrvSE.exe	8024	0	5,128	WMI Provider Host

Registry

The Windows registry is a hierarchical database that contains configuration data for the operating system, applications, and services.

1 Registry Keys

Display Name	Registry Hive	Located
XIA Configuration Server Setup	HKEY_LOCAL_MACHINE	True

1 Registry Values

Display Name	Value Type	Value	Located
XIA Configuration Server Database Name	REG_SZ	XIAConfiguration	True

XIA Configuration Server Setup

The Windows registry is a hierarchical database that contains configuration data for the operating system, applications, and services. A registry key is a container which stores registry values.

Registry Key

Located	True

Registry Key Properties

Hive	HKEY_LOCAL_MACHINE
Key Name	SOFTWARE\CENTREL Solutions\XIA Configuration Server\Setup

12 Values

Name	Value Type	Data
Account	REG_SZ	NT AUTHORITY\NETWORK SERVICE
AddUserSystemAdministrator	REG_SZ	True
AuthenticationMode	REG_SZ	NETWORKSERVICE
DatabaseInstance	REG_SZ	(local)\SQLEXPRESS
DatabaseName	REG_SZ	XIAConfiguration
Domain	REG_SZ	NT AUTHORITY
InstallDirectory	REG_SZ	C:\Program Files\CENTREL Solutions\XIA Configuration\
OrganizationName	REG_SZ	Demonstration Company
URL	REG_SZ	http://localhost/XIAConfiguration
Username	REG_SZ	NETWORK SERVICE
Version	REG_SZ	17.0.5
VIRDIR	REG_SZ	XIAConfiguration

Security

Owner	NT AUTHORITY\SYSTEM

6 Registry Permissions

Account Name	Inherited	Action	Rights	Applies To
ALL APPLICATION PACKAGES	True	Allow	Read	This key and subkeys
BUILTIN\Administrators	True	Allow	Full Control	This key and subkeys
BUILTIN\Users	True	Allow	Read	This key and subkeys
CREATOR OWNER	True	Allow	Full Control	Subkeys only
NT AUTHORITY\SYSTEM	True	Allow	Full Control	This key and subkeys
S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479	True	Allow	Read	This key and subkeys

-3232135806-4053264122 -3456934681				

0 Registry Audit Rules

There are no audit rules found.

XIA Configuration Server Database Name

The Windows registry is a hierarchical database that contains configuration data for the operating system, applications, and services. A registry value stores an individual value within a registry key.

Registry Value

Located	True

Registry Value Properties

Parent Key	HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Server\Setup
Value Name	DatabaseName
Value	XIAConfiguration
Value Type	REG_SZ

Server Roles and Features

Provides information about the Windows server roles and features such as "DNS Server" enabled on this machine. Server features are found on Windows Server 2008 and above only.

Roles and Features

Feature	Install State
☐ .NET Framework 3.5 Features	Available
☐ .NET Framework 3.5 (includes .NET 2.0 and 3.0)	Removed
☐ HTTP Activation	Available
☐ Non-HTTP Activation	Available
☑ .NET Framework 4.8 Features	Installed
☑ .NET Framework 4.8	Installed
☑ ASP.NET 4.8	Installed
☑ WCF Services	Installed
☐ HTTP Activation	Available
☐ Message Queuing (MSMQ) Activation	Available
☐ Named Pipe Activation	Available
☐ TCP Activation	Available
☑ TCP Port Sharing	Installed
☐ Active Directory Certificate Services	Available
☐ Certificate Enrollment Policy Web Service	Available
☐ Certificate Enrollment Web Service	Available
☐ Certification Authority	Available
☐ Certification Authority Web Enrollment	Available
☐ Network Device Enrollment Service	Available
☐ Online Responder	Available
☐ Active Directory Domain Services	Available
☐ Active Directory Federation Services	Available
☐ Active Directory Lightweight Directory Services	Available
☐ Active Directory Rights Management Services	Available
☐ Active Directory Rights Management Server	Available
☐ Identity Federation Support	Available
☐ Background Intelligent Transfer Service (BITS)	Available
☐ Compact Server	Available
☐ IIS Server Extension	Available
☐ BitLocker Drive Encryption	Available
☐ BitLocker Network Unlock	Available
☐ BranchCache	Available
☐ Client for NFS	Available

☐ Containers	Available
☐ Data Center Bridging	Available
☐ Device Health Attestation	Available
☐ DHCP Server	Available
☐ Direct Play	Available
☐ DNS Server	Available
☐ Enhanced Storage	Available
☐ Failover Clustering	Available
☐ Fax Server	Available
☑ File and Storage Services	Installed
☐ File and iSCSI Services	Available
☐ BranchCache for Network Files	Available
☐ Data Deduplication	Available
☐ DFS Namespaces	Available
☐ DFS Replication	Available
☐ File Server	Available
☐ File Server Resource Manager	Available
☐ File Server VSS Agent Service	Available
☐ iSCSI Target Server	Available
☐ iSCSI Target Storage Provider (VDS and VSS hardware providers)	Available
☐ Server for NFS	Available
☐ Work Folders	Available
☑ Storage Services	Installed
☑ Group Policy Management	Installed
☐ Host Guardian Hyper-V Support	Available
☐ Host Guardian Service	Available
☐ Hyper-V	Available
☐ I/O Quality of Service	Available
☐ IIS Hostable Web Core	Available
☐ Internet Printing Client	Available
☐ IP Address Management (IPAM) Server	Available
☐ LPR Port Monitor	Available
☐ Management OData IIS Extension	Available
☐ Media Foundation	Available
☐ Message Queuing	Available
☐ Message Queuing DCOM Proxy	Available
☐ Message Queuing Services	Available
☐ Directory Service Integration	Available
☐ HTTP Support	Available
☐ Message Queuing Server	Available

☐ Message Queuing Triggers	Available
☐ Multicasting Support	Available
☐ Routing Service	Available
☑ Microsoft Defender Antivirus	Installed
☐ Multipath I/O	Available
☐ MultiPoint Connector	Available
☐ MultiPoint Connector Services	Available
☐ MultiPoint Manager and MultiPoint Dashboard	Available
☐ Network ATC	Available
☐ Network Controller	Available
☐ Network Load Balancing	Available
☐ Network Policy and Access Services	Available
☐ Network Virtualization	Available
☐ Print and Document Services	Available
☐ Internet Printing	Available
☐ LPD Service	Available
☐ Print Server	Available
☐ Quality Windows Audio Video Experience	Available
☐ RAS Connection Manager Administration Kit (CMAK)	Available
☐ Remote Access	Available
☐ DirectAccess and VPN (RAS)	Available
☐ Routing	Available
☐ Web Application Proxy	Available
☐ Remote Assistance	Available
☐ Remote Desktop Services	Available
☐ Remote Desktop Connection Broker	Available
☐ Remote Desktop Gateway	Available
☐ Remote Desktop Licensing	Available
☐ Remote Desktop Session Host	Available
☐ Remote Desktop Virtualization Host	Available
☐ Remote Desktop Web Access	Available
☐ Remote Differential Compression	Available
☑ Remote Server Administration Tools	Installed
☐ Feature Administration Tools	Available
☐ BitLocker Drive Encryption Administration Utilities	Available
☐ BitLocker Drive Encryption Tools	Available
☐ BitLocker Recovery Password Viewer	Available
☐ BITS Server Extensions Tools	Available
☐ DataCenterBridging LLDP Tools	Available
☐ Failover Clustering Tools	Available

☐ Failover Cluster Automation Server	Available
☐ Failover Cluster Command Interface	Available
☐ Failover Cluster Management Tools	Available
☐ Failover Cluster Module for Windows PowerShell	Available
☐ IP Address Management (IPAM) Client	Available
☐ Network Load Balancing Tools	Available
☐ Shielded VM Tools	Available
☐ SNMP Tools	Available
☐ Storage Migration Service Tools	Available
☐ Storage Replica Module for Windows PowerShell	Available
☐ System Insights Module for Windows PowerShell	Available
☐ WINS Server Tools	Available
☑ Role Administration Tools	Installed
☐ Active Directory Certificate Services Tools	Available
☐ Certification Authority Management Tools	Available
☐ Online Responder Tools	Available
☐ Active Directory Rights Management Services Tools	Available
☑ AD DS and AD LDS Tools	Installed
☑ Active Directory module for Windows PowerShell	Installed
☐ AD DS Tools	Available
☐ Active Directory Administrative Center	Available
☐ AD DS Snap-Ins and Command-Line Tools	Available
☐ AD LDS Snap-Ins and Command-Line Tools	Available
☐ DHCP Server Tools	Available
☐ DNS Server Tools	Available
☐ Fax Server Tools	Available
☑ File Services Tools	Installed
☑ DFS Management Tools	Installed
☐ File Server Resource Manager Tools	Available
☐ Services for Network File System Management Tools	Available
☐ Hyper-V Management Tools	Available
☐ Hyper-V GUI Management Tools	Available
☐ Hyper-V Module for Windows PowerShell	Available
☐ Network Controller Management Tools	Available
☐ Network Policy and Access Services Tools	Available
☐ Print and Document Services Tools	Available
☐ Remote Access Management Tools	Available
☐ Remote Access GUI and Command-Line Tools	Available
☐ Remote Access module for Windows PowerShell	Available
☐ Remote Desktop Services Tools	Available

☐ Remote Desktop Gateway Tools	Available
☐ Remote Desktop Licensing Diagnoser Tools	Available
☐ Remote Desktop Licensing Tools	Available
☐ Volume Activation Tools	Available
☐ Windows Deployment Services Tools	Available
☐ Windows Server Update Services Tools	Available
☐ API and PowerShell cmdlets	Available
☐ User Interface Management Console	Available
☐ RPC over HTTP Proxy	Available
☐ Setup and Boot Event Collection	Available
☐ Simple TCP/IP Services	Available
☐ SMB 1.0/CIFS File Sharing Support	Available
☐ SMB 1.0/CIFS Client	Available
☐ SMB 1.0/CIFS Server	Available
☐ SMB Bandwidth Limit	Available
☐ SNMP Service	Available
☐ SNMP WMI Provider	Available
☐ Software Load Balancer	Available
☐ Storage Migration Service	Available
☐ Storage Migration Service Proxy	Available
☐ Storage Replica	Available
☑ System Data Archiver	Installed
☐ System Insights	Available
☐ Telnet Client	Available
☐ TFTP Client	Available
☐ VM Shielding Tools for Fabric Management	Available
☐ Volume Activation Services	Available
☑ Web Server (IIS)	Installed
☐ FTP Server	Available
☐ FTP Extensibility	Available
☐ FTP Service	Available
☑ Management Tools	Installed
☐ IIS 6 Management Compatibility	Available
☐ IIS 6 Metabase Compatibility	Available
☐ IIS 6 Scripting Tools	Available
☐ IIS 6 WMI Compatibility	Available
☑ IIS Management Console	Installed
☑ IIS Management Scripts and Tools	Installed
☑ Management Service	Installed
☑ Web Server	Installed

☑ Application Development	Installed
☐ .NET Extensibility 3.5	Available
☑ .NET Extensibility 4.8	Installed
☑ Application Initialization	Installed
☐ ASP	Available
☐ ASP.NET 3.5	Available
☑ ASP.NET 4.8	Installed
☐ CGI	Available
☑ ISAPI Extensions	Installed
☑ ISAPI Filters	Installed
☐ Server Side Includes	Available
☐ WebSocket Protocol	Available
☑ Common HTTP Features	Installed
☑ Default Document	Installed
☑ Directory Browsing	Installed
☑ HTTP Errors	Installed
☐ HTTP Redirection	Available
☑ Static Content	Installed
☐ WebDAV Publishing	Available
☑ Health and Diagnostics	Installed
☐ Custom Logging	Available
☑ HTTP Logging	Installed
☐ Logging Tools	Available
☐ ODBC Logging	Available
☑ Request Monitor	Installed
☐ Tracing	Available
☑ Performance	Installed
☐ Dynamic Content Compression	Available
☑ Static Content Compression	Installed
☑ Security	Installed
☐ Basic Authentication	Available
☐ Centralized SSL Certificate Support	Available
☐ Client Certificate Mapping Authentication	Available
☐ Digest Authentication	Available
☐ IIS Client Certificate Mapping Authentication	Available
☐ IP and Domain Restrictions	Available
☑ Request Filtering	Installed
☐ URL Authorization	Available
☑ Windows Authentication	Installed
☐ WebDAV Redirector	Available

☑ Windows Admin Center Setup	Installed
☐ Windows Biometric Framework	Available
☐ Windows Deployment Services	Available
☐ Deployment Server	Available
☐ Transport Server	Available
☐ Windows Identity Foundation 3.5	Available
☐ Windows Internal Database	Available
☑ Windows PowerShell	Installed
☐ Windows PowerShell 2.0 Engine	Removed
☑ Windows PowerShell 5.1	Installed
☐ Windows PowerShell Desired State Configuration Service	Available
☐ Windows PowerShell Web Access	Available
☑ Windows Process Activation Service	Installed
☐ .NET Environment 3.5	Available
☑ Configuration APIs	Installed
☑ Process Model	Installed
☐ Windows Search Service	Available
☐ Windows Server Backup	Available
☐ Windows Server Migration Tools	Available
☐ Windows Server Update Services	Available
☐ SQL Server Connectivity	Available
☐ WID Connectivity	Available
☐ WSUS Services	Available
☐ Windows Standards-Based Storage Management	Available
☐ Windows Subsystem for Linux	Available
☐ Windows TIFF IFilter	Available
☐ WinRM IIS Extension	Available
☐ WINS Server	Available
☑ Wireless LAN Service	Installed
☑ WoW64 Support	Installed
☑ XPS Viewer	Installed

Startup Commands

Provides information about the commands configured to run at startup for the users of this Windows machine.

AzureArcSetup

Command	%windir%\AzureArcSetup\Systray\AzureArcSysTray.exe
Location	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User	Public

SecurityHealth

Command	%windir%\system32\SecurityHealthSystray.exe
Location	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User	Public

VMware User Process

Command	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
Location	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User	Public

Task Scheduler Library

The Task Scheduler Library automates tasks that perform actions at a specific time or when a certain event occurs and replaces Scheduled Tasks on previous versions of Windows.

4 Scheduled Tasks

Name	Triggers	Account Name
GoogleUpdaterTaskSystem134.0.6985.0{B3D23309-EFDA-4690-81D4-60EE802797D6}	Multiple triggers defined	NT AUTHORITY\SYSTEM
MicrosoftEdgeUpdateTaskMachineCore{408EE469-8D4F-4D4C-ADED-421EB55AD459}	Multiple triggers defined	NT AUTHORITY\SYSTEM
MicrosoftEdgeUpdateTaskMachineUA{4165CA3F-A67B-4CE8-BEDC-06ABB9DE3E90}	At 5:15 PM every day	NT AUTHORITY\SYSTEM
Process Explorer-CONTOSO-sysadmin	At log on of CONTOSO\sysadmin	CONTOSO\sysadmin

GoogleUpdaterTaskSystem134.0.6985.0{B3D23309-EFDA-4690-81D4-60EE802797D6}

GoogleUpdater Task System 134.0.6985.0

General

Name	GoogleUpdaterTaskSystem134.0.6985.0{B3D23309-EFDA-4690-81D4-60EE802797D6}
Task Path	\GoogleSystem\GoogleUpdater
Author	NT AUTHORITY\SYSTEM
Enabled	True
Hidden	True
Version	Windows Vista™ or Windows Server™ 2008

Security

Account Name	NT AUTHORITY\SYSTEM
Logon Type	Run whether user is logged on or not (service).
Use Highest Privileges	True

Settings

Allow Task To Be Run On Demand	True
Run After Missed Scheduled Start	True
Task Failure Restart	Do not restart
Execution Time Limit	Stop the task if it runs longer than 3 days
Force Terminate Tasks	True
Delete Expired Task	Do not delete
Multiple Instance Action	Do not start a new instance

Conditions

Idle Duration	Do not wait for the computer to become idle
Disallow Start On Batteries	False
Wake Computer To Run Task	False
Network Requirement	None

Execute Action

Command	"C:\Program Files (x86)\Google\GoogleUpdater\134.0.6985.0\updater.exe"
Arguments	--wake --system
Working Directory	

At log on

Summary	At log on of any user
Delay Task	No delay
Repetition	No repetition
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Activate Task	[Not Configured]
Activate Task (Synchronize)	False
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

On specified schedule

Summary	At 3:46 PM every day
Delay Task	No delay
Repetition	Repeat the task every 1 hour for 1 day
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

MicrosoftEdgeUpdateTaskMachineCore{408EE469-8D4F-4D4C-ADED-421EB55AD459}

Keeps your Microsoft software up to date. If this task is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This task uninstalls itself when there is no Microsoft software using it.

General

Name	MicrosoftEdgeUpdateTaskMachineCore{408EE469-8D4F-4D4C-ADED-421EB55AD459}
Task Path	\
Author	
Enabled	True
Hidden	False
Version	Windows Vista™ or Windows Server™ 2008

Security

Account Name	NT AUTHORITY\SYSTEM
Logon Type	Run whether user is logged on or not (service).
Use Highest Privileges	True

Settings

Allow Task To Be Run On Demand	True
Run After Missed Scheduled Start	True
Task Failure Restart	Do not restart
Execution Time Limit	Stop the task if it runs longer than 3 days
Force Terminate Tasks	True
Delete Expired Task	Do not delete
Multiple Instance Action	Do not start a new instance

Conditions

Idle Duration	Do not wait for the computer to become idle
Disallow Start On Batteries	False
Wake Computer To Run Task	False
Network Requirement	None

Execute Action

Command	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
Arguments	/c
Working Directory	

At log on

Summary	At log on of any user
Delay Task	No delay
Repetition	No repetition
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Activate Task	[Not Configured]
Activate Task (Synchronize)	False
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

On specified schedule

Summary	At 5:45 PM every day
Delay Task	No delay
Repetition	No repetition
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

MicrosoftEdgeUpdateTaskMachineUA{4165CA3F-A67B-4CE8-BEDC-06ABB9DE3E90}

Keeps your Microsoft software up to date. If this task is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This task uninstalls itself when there is no Microsoft software using it.

General

Name	MicrosoftEdgeUpdateTaskMachineUA{4165CA3F-A67B-4CE8-BEDC-06ABB9DE3E90}
Task Path	\
Author	
Enabled	True
Hidden	False
Version	Windows Vista™ or Windows Server™ 2008

Security

Account Name	NT AUTHORITY\SYSTEM
Logon Type	Run whether user is logged on or not (service).
Use Highest Privileges	True

Settings

Allow Task To Be Run On Demand	True
Run After Missed Scheduled Start	True
Task Failure Restart	Do not restart
Execution Time Limit	Stop the task if it runs longer than 3 days
Force Terminate Tasks	True
Delete Expired Task	Do not delete
Multiple Instance Action	Do not start a new instance

Conditions

Idle Duration	Do not wait for the computer to become idle
Disallow Start On Batteries	False
Wake Computer To Run Task	False
Network Requirement	None

Execute Action

Command	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
Arguments	/ua /installsource scheduler
Working Directory	

On specified schedule

Summary	At 5:15 PM every day
Delay Task	No delay
Repetition	Repeat the task every 1 hour for 1 day
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

Process Explorer-CONTOSO-sysadmin

Scheduled tasks can be used to schedule commands, programs, or scripts to run at specific times.

General

Name	Process Explorer-CONTOSO-sysadmin
Task Path	\
Author	Process Explorer
Enabled	True
Hidden	False
Version	Windows Vista™ or Windows Server™ 2008

Security

Account Name	CONTOSO\sysadmin
Logon Type	Run only when a user is logged on.
Use Highest Privileges	False

Settings

Allow Task To Be Run On Demand	True
Run After Missed Scheduled Start	True
Task Failure Restart	Do not restart
Execution Time Limit	Stop the task if it runs longer than 3 days
Force Terminate Tasks	True
Delete Expired Task	Do not delete
Multiple Instance Action	Do not start a new instance

Conditions

Idle Duration	Do not wait for the computer to become idle
Disallow Start On Batteries	False
Wake Computer To Run Task	False
Network Requirement	None

Execute Action

Command	"C:\PROCESSEXPLORER\PROCEXP64.EXE"
Arguments	/t
Working Directory	

At log on

Summary	At log on of CONTOSO\sysadmin
Delay Task	No delay
Repetition	No repetition
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Activate Task	[Not Configured]
Activate Task (Synchronize)	False
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

Windows Remote Management (WinRM)

Windows Remote Management (WinRM) is the Microsoft implementation of the WS-MAN management protocol, and the underlying communication technology used by PowerShell remoting.

Service Settings

Allow Remote Server Management	True
Allow Unencrypted Traffic	False
Channel Binding Token Hardening	Relaxed
Disallow Storing RunAs Credentials	False
IPv4 Filter	*
IPv6 Filter	*
Started	True
Use HTTP Compatibility Listener	False
Use HTTPS Compatibility Listener	False
Version	10.0.26100.1

Service Authentication Settings

Allow Basic Authentication	False
Allow CredSSP Authentication	False
Allow Kerberos Authentication	True
Allow Negotiate Authentication	True

Listener Listener_1084132640

Enabled	True
Address	*
Port	5985
Protocol	HTTP
URI Prefix	wsman

Client Settings

Allow Unencrypted Traffic	False
Default HTTP Port	5985
Default HTTPS Port	5986
Trusted Hosts	*
Trusted Hosts Source	Configured Locally

Client Authentication Settings

Allow Basic Authentication	True
Allow CredSSP Authentication	False
Allow Digest Authentication	True
Allow Kerberos Authentication	True
Allow Negotiate Authentication	True

Windows Remote Shell

Allow Remote Shell Access	True
Allow Remote Shell Access Source	Not Defined
Idle Timeout (ms)	7,200,000
Maximum Concurrent Users	2,147,483,647
Maximum Memory Per Shell (MB)	2,147,483,647
Maximum Processes Per Shell	2,147,483,647
Maximum Shells Per User	2,147,483,647

Windows Services

Displays the configuration of the Windows services on this machine

250 Windows Services

Display Name	Start Mode	Account Name
ActiveX Installer (AxInstSV)	Manual	LocalSystem
App Readiness	Manual	LocalSystem
Application Host Helper Service	Automatic	localSystem
Application Identity	Manual (Trigger Start)	NT Authority\LocalService
Application Information	Manual (Trigger Start)	LocalSystem
Application Layer Gateway Service	Manual	NT AUTHORITY\LocalService
Application Management	Manual	LocalSystem
AppX Deployment Service (AppXSVC)	Manual (Trigger Start)	LocalSystem
ASP.NET State Service	Manual	NT AUTHORITY\NetworkService
Auto Time Zone Updater	Disabled	NT AUTHORITY\LocalService
AzureAttestService	Automatic	LocalSystem
Background Intelligent Transfer Service	Automatic (Delayed Start)	LocalSystem
Background Tasks Infrastructure Service	Automatic	LocalSystem
Base Filtering Engine	Automatic	NT AUTHORITY\LocalService
Bluetooth Support Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
BluetoothUserService_1c2dca	Manual (Trigger Start)	
BTAGService	Manual (Trigger Start)	NT AUTHORITY\LocalService
BthAvctpSvc	Manual (Trigger Start)	NT AUTHORITY\LocalService
Capability Access Manager Service	Manual (Trigger Start)	LocalSystem
CaptureService_1c2dca	Manual	

Certificate Propagation	Manual (Trigger Start)	LocalSystem
Client License Service (ClipSVC)	Manual (Trigger Start)	LocalSystem
Clipboard User Service_1c2dca	Automatic	
CloudBackupRestoreSvc_1c2dca	Manual	
CNG Key Isolation	Manual (Trigger Start)	LocalSystem
COM+ Event System	Automatic	NT AUTHORITY\LocalService
COM+ System Application	Manual	LocalSystem
Connected Devices Platform Service	Automatic (Delayed Start, Trigger Start)	NT AUTHORITY\LocalService
Connected Devices Platform User Service_1c2dca	Automatic	
Connected User Experiences and Telemetry	Automatic	LocalSystem
ConsentUX User Service_1c2dca	Manual	
Contact Data_1c2dca	Manual	
CoreMessaging	Automatic	NT AUTHORITY\LocalService
Credential Manager	Manual	LocalSystem
CredentialEnrollmentManagerUserSvc_1c2dca	Manual	
Cryptographic Services	Automatic (Trigger Start)	NT Authority\NetworkService
Data Sharing Service	Manual (Trigger Start)	LocalSystem
DCOM Server Process Launcher	Automatic	LocalSystem
Declared Configuration(DC) service	Manual (Trigger Start)	LocalSystem
Delivery Optimization	Manual (Trigger Start)	NT Authority\NetworkService
Device Association Service	Manual (Trigger Start)	LocalSystem
Device Install Service	Manual (Trigger Start)	LocalSystem
Device Management Enrollment Service	Manual	LocalSystem
Device Management Wireless Application Protocol (WAP) Push message Routing Service	Manual (Trigger Start)	LocalSystem
Device Setup Manager	Manual (Trigger Start)	LocalSystem
DeviceAssociationBroker_1c2dca	Manual	

DevicePicker_1c2dca	Manual	
DevicesFlow_1c2dca	Manual	
DevQuery Background Discovery Broker	Manual (Trigger Start)	LocalSystem
DHCP Client	Automatic	NT Authority\LocalService
Diagnostic Policy Service	Automatic (Delayed Start)	NT AUTHORITY\LocalService
Diagnostic Service Host	Manual	NT AUTHORITY\LocalService
Diagnostic System Host	Manual	LocalSystem
Display Policy Service	Automatic	NT AUTHORITY\LocalService
DisplayEnhancementService	Manual (Trigger Start)	LocalSystem
Distributed Link Tracking Client	Automatic	LocalSystem
Distributed Transaction Coordinator	Automatic (Delayed Start)	NT AUTHORITY\NetworkService
DNS Client	Automatic (Trigger Start)	NT AUTHORITY\NetworkService
Downloaded Maps Manager	Disabled	NT AUTHORITY\NetworkService
Embedded Mode	Manual (Trigger Start)	LocalSystem
Encrypting File System (EFS)	Manual (Trigger Start)	LocalSystem
Enterprise App Management Service	Manual	LocalSystem
Extensible Authentication Protocol	Manual	localSystem
Function Discovery Provider Host	Manual	NT AUTHORITY\LocalService
Function Discovery Resource Publication	Manual (Trigger Start)	NT AUTHORITY\LocalService
GameInput Service	Manual (Trigger Start)	LocalSystem
Geolocation Service	Manual (Trigger Start)	LocalSystem
Google Chrome Elevation Service (GoogleChromeElevationService)	Manual	LocalSystem
Google Updater Internal Service (GoogleUpdaterInternalService134.0.6985.0)	Automatic	LocalSystem
Google Updater Service (GoogleUpdaterService134.0.6985.0)	Automatic	LocalSystem
GraphicsPerfSvc	Manual (Trigger Start)	LocalSystem
Group Policy Client	Automatic (Trigger Start)	LocalSystem

Human Interface Device Service	Manual (Trigger Start)	LocalSystem
HV Host Service	Manual (Trigger Start)	LocalSystem
Hyper-V Data Exchange Service	Manual (Trigger Start)	LocalSystem
Hyper-V Guest Service Interface	Manual (Trigger Start)	LocalSystem
Hyper-V Guest Shutdown Service	Manual (Trigger Start)	LocalSystem
Hyper-V Heartbeat Service	Manual (Trigger Start)	LocalSystem
Hyper-V PowerShell Direct Service	Manual (Trigger Start)	LocalSystem
Hyper-V Remote Desktop Virtualization Service	Manual (Trigger Start)	LocalSystem
Hyper-V Time Synchronization Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
Hyper-V Volume Shadow Copy Requestor	Manual (Trigger Start)	LocalSystem
IKE and AuthIP IPsec Keying Modules	Manual (Trigger Start)	LocalSystem
Internet Connection Sharing (ICS)	Manual (Trigger Start)	LocalSystem
Inventory and Compatibility Appraisal service	Automatic (Delayed Start)	LocalSystem
IP Helper	Automatic	LocalSystem
IPsec Policy Agent	Manual (Trigger Start)	NT Authority\NetworkService
KDC Proxy Server service (KPS)	Manual	NT AUTHORITY\NetworkService
Kerberos Local Key Distribution Center	Automatic	LocalSystem
KtmRm for Distributed Transaction Coordinator	Manual (Trigger Start)	NT AUTHORITY\NetworkService
Link-Layer Topology Discovery Mapper	Manual	NT AUTHORITY\LocalService
Local Session Manager	Automatic	LocalSystem
LxpSvc	Manual	LocalSystem
McpManagementService	Manual	LocalSystem
Microsoft Account Sign-in Assistant	Manual (Trigger Start)	LocalSystem
Microsoft App-V Client	Disabled	LocalSystem
Microsoft Defender Antivirus Network Inspection Service	Manual	NT AUTHORITY\LocalService
Microsoft Defender Antivirus Service	Manual	LocalSystem

Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)	Manual	LocalSystem
Microsoft Edge Update Service (edgeupdate)	Automatic (Delayed Start, Trigger Start)	LocalSystem
Microsoft Edge Update Service (edgeupdatem)	Manual (Trigger Start)	LocalSystem
Microsoft iSCSI Initiator Service	Manual	LocalSystem
Microsoft Software Shadow Copy Provider	Manual	LocalSystem
Microsoft Storage Spaces SMP	Manual	NT AUTHORITY\NetworkService
Microsoft Store Install Service	Manual	LocalSystem
NaturalAuthentication	Manual (Trigger Start)	LocalSystem
Net.Tcp Port Sharing Service	Disabled	NT AUTHORITY\LocalService
Netlogon	Automatic	LocalSystem
Network Connection Broker	Manual (Trigger Start)	LocalSystem
Network Connections	Manual	LocalSystem
Network Connectivity Assistant	Manual (Trigger Start)	LocalSystem
Network List Service	Manual	NT AUTHORITY\NetworkService
Network Location Awareness	Manual	NT AUTHORITY\NetworkService
Network Setup Service	Manual (Trigger Start)	LocalSystem
Network Store Interface Service	Automatic	NT Authority\LocalService
NgcCtnrSvc	Manual (Trigger Start)	NT AUTHORITY\LocalService
NgcSvc	Manual (Trigger Start)	LocalSystem
Now Playing Session Manager Service_1c2dca	Manual	
Offline Files	Disabled	LocalSystem
OpenSSH Authentication Agent	Disabled	LocalSystem
OpenSSH SSH Server	Manual	LocalSystem
Optimize drives	Manual	localSystem
P9RdrService_1c2dca	Manual (Trigger Start)	
Payments and NFC/SE Manager	Manual (Trigger Start)	NT AUTHORITY\LocalService

Performance Counter DLL Host	Manual	NT AUTHORITY\LocalService
Performance Logs & Alerts	Manual	NT AUTHORITY\LocalService
Plug and Play	Manual	LocalSystem
Portable Device Enumerator Service	Manual (Trigger Start)	LocalSystem
Power	Automatic	LocalSystem
Print Device Configuration Service	Manual (Trigger Start)	LocalSystem
Print Spooler	Automatic	LocalSystem
Printer Extensions and Notifications	Manual	LocalSystem
PrintScanBrokerService	Manual	LocalSystem
PrintWorkflow_1c2dca	Manual (Trigger Start)	
Problem Reports Control Panel Support	Manual	localSystem
Program Compatibility Assistant Service	Automatic (Delayed Start, Trigger Start)	LocalSystem
Quality Windows Audio Video Experience	Manual	NT AUTHORITY\LocalService
Radio Management Service	Manual	NT AUTHORITY\LocalService
ReFS Dedup Service	Manual	LocalSystem
Remote Access Auto Connection Manager	Manual	localSystem
Remote Access Connection Manager	Manual	localSystem
Remote Desktop Configuration	Manual	localSystem
Remote Desktop Services	Manual	NT Authority\NetworkService
Remote Desktop Services UserMode Port Redirector	Manual	localSystem
Remote Procedure Call (RPC)	Automatic	NT AUTHORITY\NetworkService
Remote Procedure Call (RPC) Locator	Manual	NT AUTHORITY\NetworkService
Remote Registry	Automatic (Trigger Start)	NT AUTHORITY\LocalService
Resultant Set of Policy Provider	Manual	LocalSystem
Routing and Remote Access	Disabled	localSystem
RPC Endpoint Mapper	Automatic	NT AUTHORITY\NetworkService

Secondary Logon	Manual	LocalSystem
Secure Socket Tunneling Protocol Service	Manual	NT Authority\LocalService
Security Accounts Manager	Automatic	LocalSystem
Sensor Data Service	Manual (Trigger Start)	LocalSystem
Sensor Monitoring Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
Sensor Service	Manual (Trigger Start)	LocalSystem
Server	Automatic (Trigger Start)	LocalSystem
Shared PC Account Manager	Disabled	LocalSystem
Shell Hardware Detection	Automatic	LocalSystem
Smart Card	Manual (Trigger Start)	NT AUTHORITY\LocalService
Smart Card Device Enumeration Service	Manual (Trigger Start)	LocalSystem
Smart Card Removal Policy	Manual	LocalSystem
SNMP Trap	Manual	NT AUTHORITY\LocalService
Software Protection	Automatic (Delayed Start, Trigger Start)	NT AUTHORITY\NetworkService
Special Administration Console Helper	Manual	LocalSystem
Spot Verifier	Manual (Trigger Start)	LocalSystem
SQL Server (SQLEXPRESS)	Automatic (Delayed Start)	NT Service\MSSQL$SQLEXPRESS
SQL Server Agent (SQLEXPRESS)	Disabled	NT AUTHORITY\NETWORKSERVICE
SQL Server Browser	Disabled	NT AUTHORITY\LOCALSERVICE
SQL Server CEIP service (SQLEXPRESS)	Automatic (Delayed Start)	NT Service\SQLTELEMETRY$SQLEXPRESS
SQL Server VSS Writer	Automatic	LocalSystem
SSDP Discovery	Disabled	NT AUTHORITY\LocalService
State Repository Service	Automatic	LocalSystem
Still Image Acquisition Events	Manual	LocalSystem
Storage Service	Automatic (Delayed Start, Trigger Start)	LocalSystem
Storage Tiers Management	Manual	localSystem

Sync Host_1c2dca	Automatic	
SysMain	Automatic	LocalSystem
System Event Notification Service	Automatic	LocalSystem
System Events Broker	Automatic (Trigger Start)	LocalSystem
System Guard Runtime Monitor Broker	Disabled	LocalSystem
Task Scheduler	Automatic	LocalSystem
TCP/IP NetBIOS Helper	Manual (Trigger Start)	NT AUTHORITY\LocalService
Telephony	Manual	NT AUTHORITY\NetworkService
Text Input Management Service	Automatic (Trigger Start)	LocalSystem
Themes	Automatic	LocalSystem
Time Broker	Manual (Trigger Start)	NT AUTHORITY\LocalService
Udk User Service_1c2dca	Manual	
Update Orchestrator Service	Automatic (Delayed Start)	LocalSystem
UPnP Device Host	Disabled	NT AUTHORITY\LocalService
User Access Logging Service	Automatic (Delayed Start)	LocalSystem
User Data Access_1c2dca	Manual	
User Data Storage_1c2dca	Manual	
User Experience Virtualization Service	Disabled	LocalSystem
User Manager	Automatic (Trigger Start)	LocalSystem
User Profile Service	Automatic	LocalSystem
Virtual Disk	Manual	LocalSystem
VMware Alias Manager and Ticket Service	Automatic	LocalSystem
VMware Snapshot Provider	Manual	LocalSystem
VMware SVGA Helper Service	Automatic	LocalSystem
VMware Tools	Automatic	LocalSystem
Volume Shadow Copy	Manual	LocalSystem

W3C Logging Service	Manual	localSystem
WaaSMedicSvc	Manual	LocalSystem
WalletService	Manual	LocalSystem
Warp JIT Service	Manual (Trigger Start)	NT Authority\LocalService
Web Account Manager	Manual	LocalSystem
Web Management Service	Manual	NT AUTHORITY\LocalService
Wi-Fi Direct Services Connection Manager Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
Windows Audio	Automatic	NT AUTHORITY\LocalService
Windows Audio Endpoint Builder	Automatic	LocalSystem
Windows Biometric Service	Manual (Trigger Start)	LocalSystem
Windows Camera Frame Server	Manual (Trigger Start)	NT AUTHORITY\LocalService
Windows Camera Frame Server Monitor	Manual (Trigger Start)	LocalSystem
Windows Connect Now - Config Registrar	Manual	NT AUTHORITY\LocalService
Windows Connection Manager	Automatic (Trigger Start)	NT Authority\LocalService
Windows Defender Advanced Threat Protection Service	Manual	LocalSystem
Windows Defender Firewall	Automatic	NT Authority\LocalService
Windows Encryption Provider Host Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
Windows Error Reporting Service	Manual (Trigger Start)	localSystem
Windows Event Collector	Manual	NT AUTHORITY\NetworkService
Windows Event Log	Automatic	NT AUTHORITY\LocalService
Windows Font Cache Service	Automatic	NT AUTHORITY\LocalService
Windows Image Acquisition (WIA)	Manual (Trigger Start)	NT Authority\LocalService
Windows Insider Service	Manual (Trigger Start)	LocalSystem
Windows Installer	Manual	LocalSystem
Windows License Manager Service	Manual (Trigger Start)	NT Authority\LocalService
Windows Management Instrumentation	Automatic	localSystem

Windows Media Player Network Sharing Service	Manual	NT AUTHORITY\NetworkService
Windows Modules Installer	Manual	localSystem
Windows Process Activation Service	Manual	localSystem
Windows Push Notifications System Service	Automatic	LocalSystem
Windows Push Notifications User Service_1c2dca	Automatic	
Windows PushToInstall Service	Manual (Trigger Start)	LocalSystem
Windows Remote Management (WS-Management)	Automatic	NT AUTHORITY\NetworkService
Windows Search	Disabled	LocalSystem
Windows Security Service	Manual	LocalSystem
Windows Time	Automatic (Trigger Start)	NT AUTHORITY\LocalService
Windows Update	Automatic (Trigger Start)	LocalSystem
WinHTTP Web Proxy Auto-Discovery Service	Manual	NT AUTHORITY\LocalService
Wired AutoConfig	Manual	localSystem
WLAN AutoConfig	Manual	LocalSystem
WManSvc	Manual	LocalSystem
WMI Performance Adapter	Manual	localSystem
Work Folders	Manual	NT AUTHORITY\LocalService
Workstation	Automatic	NT AUTHORITY\NetworkService
World Wide Web Publishing Service	Automatic	localSystem
XblAuthManager	Manual	LocalSystem
XIA Configuration Scheduler	Automatic	NT AUTHORITY\NETWORK SERVICE
XIA Configuration Service	Automatic	CONTOSO\sysadmin

Windows Services [A - I]

Displays the configuration of the Windows services on this machine

ActiveX Installer (AxInstSV)

Name	AxInstSV
Display Name	ActiveX Installer (AxInstSV)
Description	Provides User Account Control validation for the installation of ActiveX controls from the Internet and enables management of ActiveX control installation based on Group Policy settings. This service is started on demand and if disabled the installation of ActiveX controls will behave according to default browser settings.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k AxInstSVGroup
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

App Readiness

Name	AppReadiness
Display Name	App Readiness
Description	Gets apps ready for use the first time a user signs in to this PC and when adding new apps.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k AppReadiness -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Application Host Helper Service

Name	AppHostSvc
Display Name	Application Host Helper Service
Description	Provides administrative services for IIS, for example configuration history and Application Pool account mapping. If this service is stopped, configuration history and locking down files or directories with Application Pool specific Access Control Entries will not work.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k apphost
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Application Identity

Name	AppIDSvc
Display Name	Application Identity
Description	Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs AppID CryptSvc

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Application Information

Name	Appinfo
Display Name	Application Information
Description	Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform desired user tasks.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs ProfSvc

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Application Layer Gateway Service

Name	ALG
Display Name	Application Layer Gateway Service
Description	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\alg.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Application Management

Name	AppMgmt
Display Name	Application Management
Description	Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is disabled, users will be unable to install, remove, or enumerate software deployed through Group Policy. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

AppX Deployment Service (AppXSVC)

Name	AppXSvc
Display Name	AppX Deployment Service (AppXSVC)
Description	Provides infrastructure support for deploying Store applications. This service is started on demand and if disabled Store applications will not be deployed to the system, and may not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k wsappx -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss staterepository

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

ASP.NET State Service

Name	aspnet_state
Display Name	ASP.NET State Service
Description	Provides support for out-of-process session states for ASP.NET. If this service is stopped, out-of-process requests will not be processed. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Auto Time Zone Updater

Name	tzautoupdate
Display Name	Auto Time Zone Updater
Description	Automatically sets the system time zone.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

AzureAttestService

Name	AzureAttestService
Display Name	AzureAttestService
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k AzureAttestService
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Background Intelligent Transfer Service

Name	BITS
Display Name	Background Intelligent Transfer Service
Description	Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN Explorer, will be unable to automatically download programs and other information.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Background Tasks Infrastructure Service

Name	BrokerInfrastructure
Display Name	Background Tasks Infrastructure Service
Description	Windows infrastructure service that controls which background tasks can run on the system.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcEptMapper DcomLaunch RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Restart the Computer
Subsequent Failure Action	Restart the Computer
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	2 minutes

Base Filtering Engine

Name	BFE
Display Name	Base Filtering Engine
Description	The Base Filtering Engine (BFE) is a service that manages firewall and Internet Protocol security (IPsec) policies and implements user mode filtering. Stopping or disabling the BFE service will significantly reduce the security of the system. It will also result in unpredictable behavior in IPsec management and firewall applications.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Bluetooth Support Service

Name	bthserv
Display Name	Bluetooth Support Service
Description	The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed Bluetooth devices to fail to operate properly and prevent new devices from being discovered or associated.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

BluetoothUserService_1c2dca

Name	BluetoothUserService_1c2dca
Display Name	BluetoothUserService_1c2dca
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k BthAppGroup -p
Service Execution Type	Unknown
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

BTAGService

Name	BTAGService
Display Name	BTAGService
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

BthAvctpSvc

Name	BthAvctpSvc
Display Name	BthAvctpSvc
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Capability Access Manager Service

Name	camsvc
Display Name	Capability Access Manager Service
Description	Provides facilities for managing UWP apps access to app capabilities as well as checking an app's access to specific app capabilities

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k osprivacy -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

CaptureService_1c2dca

Name	CaptureService_1c2dca
Display Name	CaptureService_1c2dca
Description	Enables optional screen capture functionality for applications that call the Windows.Graphics.Capture API.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Certificate Propagation

Name	CertPropSvc
Display Name	Certificate Propagation
Description	Copies user certificates and root certificates from smart cards into the current user's certificate store, detects when a smart card is inserted into a smart card reader, and, if needed, installs the smart card Plug and Play minidriver.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Client License Service (ClipSVC)

Name	ClipSVC
Display Name	Client License Service (ClipSVC)
Description	Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled applications bought using the Microsoft Store will not behave correctly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k wsappx -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Clipboard User Service_1c2dca

Name	cbdhsvc_1c2dca
Display Name	Clipboard User Service_1c2dca
Description	This user service is used for Clipboard scenarios

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k ClipboardSvcGroup -p
Service Execution Type	Unknown
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

CloudBackupRestoreSvc_1c2dca

Name	CloudBackupRestoreSvc_1c2dca
Display Name	CloudBackupRestoreSvc_1c2dca
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

CNG Key Isolation

Name	KeyIso
Display Name	CNG Key Isolation
Description	The CNG key isolation service is hosted in the LSA process. The service provides key process isolation to private keys and associated cryptographic operations as required by the Common Criteria. The service stores and uses long-lived keys in a secure process complying with Common Criteria requirements.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\lsass.exe
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

COM+ Event System

Name	EventSystem
Display Name	COM+ Event System
Description	Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. If the service is stopped, SENS will close and will not be able to provide logon and logoff notifications. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

COM+ System Application

Name	COMSysApp
Display Name	COM+ System Application
Description	Manages the configuration and tracking of Component Object Model (COM)+-based components. If the service is stopped, most COM+-based components will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	RpcSs EventSystem SENS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Connected Devices Platform Service

Name	CDPSvc
Display Name	Connected Devices Platform Service
Description	This service is used for Connected Devices Platform scenarios

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Running

Dependencies

Service Depends On	ncbservice RpcSS Tcpip

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Connected Devices Platform User Service_1c2dca

Name	CDPUserSvc_1c2dca
Display Name	Connected Devices Platform User Service_1c2dca
Description	This user service is used for Connected Devices Platform scenarios

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Connected User Experiences and Telemetry

Name	DiagTrack
Display Name	Connected User Experiences and Telemetry
Description	The Connected User Experiences and Telemetry service enables features that support in-application and connected user experiences. Additionally, this service manages the event driven collection and transmission of diagnostic and usage information (used to improve the experience and quality of the Windows Platform) when the diagnostics and usage privacy option settings are enabled under Feedback and Diagnostics.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k utcsvc -p
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

ConsentUX User Service_1c2dca

Name	ConsentUxUserSvc_1c2dca
Display Name	ConsentUX User Service_1c2dca
Description	Allows the system to request user consent to allow apps to access sensitive resources and information such as the device's location

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DevicesFlow
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Contact Data_1c2dca

Name	PimIndexMaintenanceSvc_1c2dca
Display Name	Contact Data_1c2dca
Description	Indexes contact data for fast contact searching. If you stop or disable this service, contacts might be missing from your search results.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

CoreMessaging

Name	CoreMessagingRegistrar
Display Name	CoreMessaging
Description	Manages communication between system components.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	True
Computer Restart Delay	0 minutes

Credential Manager

Name	VaultSvc
Display Name	Credential Manager
Description	Provides secure storage and retrieval of credentials to users, applications and security service packages.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\lsass.exe
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

CredentialEnrollmentManagerUserSvc_1c2dca

Name	CredentialEnrollmentManagerUserSvc_1c2dca
Display Name	CredentialEnrollmentManagerUserSvc_1c2dca
Description	Credential Enrollment Manager

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\CredentialEnrollmentManager.exe
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Cryptographic Services

Name	CryptSvc
Display Name	Cryptographic Services
Description	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as SSL. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k NetworkService -p
Service Execution Type	Own Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT Authority\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Data Sharing Service

Name	DsSvc
Display Name	Data Sharing Service
Description	Provides data brokering between applications.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

DCOM Server Process Launcher

Name	DcomLaunch
Display Name	DCOM Server Process Launcher
Description	The DCOMLAUNCH service launches COM and DCOM servers in response to object activation requests. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the DCOMLAUNCH service running.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	1 minutes

Declared Configuration(DC) service

Name	dcsvc
Display Name	Declared Configuration(DC) service
Description	Process Declared Configuration documents recevied from MDM and other channels and perform configurations on device

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Delivery Optimization

Name	DoSvc
Display Name	Delivery Optimization
Description	Performs content delivery optimization tasks

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k NetworkService -p
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT Authority\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Device Association Service

Name	DeviceAssociationService
Display Name	Device Association Service
Description	Enables pairing between the system and wired or wireless devices.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Device Install Service

Name	DeviceInstall
Display Name	Device Install Service
Description	Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	True

Device Management Enrollment Service

Name	DmEnrollmentSvc
Display Name	Device Management Enrollment Service
Description	Performs Device Enrollment Activities for Device Management

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Device Management Wireless Application Protocol (WAP) Push message Routing Service

Name	dmwappushservice
Display Name	Device Management Wireless Application Protocol (WAP) Push message Routing Service
Description	Routes Wireless Application Protocol (WAP) Push messages received by the device and synchronizes Device Management sessions

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Device Setup Manager

Name	DsmSvc
Display Name	Device Setup Manager
Description	Enables the detection, download and installation of device-related software. If this service is disabled, devices may be configured with outdated software, and may not work correctly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

DeviceAssociationBroker_1c2dca

Name	DeviceAssociationBrokerSvc_1c2dca
Display Name	DeviceAssociationBroker_1c2dca
Description	Enables apps to pair devices

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DevicesFlow -p
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

DevicePicker_1c2dca

Name	DevicePickerUserSvc_1c2dca
Display Name	DevicePicker_1c2dca
Description	This user service is used for managing the Miracast, DLNA, and DIAL UI

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DevicesFlow
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

DevicesFlow_1c2dca

Name	DevicesFlowUserSvc_1c2dca
Display Name	DevicesFlow_1c2dca
Description	Allows ConnectUX and PC Settings to Connect and Pair with WiFi displays and Bluetooth devices.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DevicesFlow
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

DevQuery Background Discovery Broker

Name	DevQueryBroker
Display Name	DevQuery Background Discovery Broker
Description	Enables apps to discover devices with a backgroud task

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

DHCP Client

Name	Dhcp
Display Name	DHCP Client
Description	Registers and updates IP addresses and DNS records for this computer. If this service is stopped, this computer will not receive dynamic IP addresses and DNS updates. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	NSI Afd

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Diagnostic Policy Service

Name	DPS
Display Name	Diagnostic Policy Service
Description	The Diagnostic Policy Service enables problem detection, troubleshooting and resolution for Windows components. If this service is stopped, diagnostics will no longer function.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalServiceNoNetwork -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Diagnostic Service Host

Name	WdiServiceHost
Display Name	Diagnostic Service Host
Description	The Diagnostic Service Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local Service context. If this service is stopped, any diagnostics that depend on it will no longer function.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Diagnostic System Host

Name	WdiSystemHost
Display Name	Diagnostic System Host
Description	The Diagnostic System Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local System context. If this service is stopped, any diagnostics that depend on it will no longer function.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Display Policy Service

Name	DispBrokerDesktopSvc
Display Name	Display Policy Service
Description	Manages the connection and configuration of local and remote displays

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSS

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

DisplayEnhancementService

Name	DisplayEnhancementService
Display Name	DisplayEnhancementService
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Distributed Link Tracking Client

Name	TrkWks
Display Name	Distributed Link Tracking Client
Description	Maintains links between NTFS files within a computer or across computers in a network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Distributed Transaction Coordinator

Name	MSDTC
Display Name	Distributed Transaction Coordinator
Description	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will fail. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\msdtc.exe
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	RPCSS SamSS

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

DNS Client

Name	Dnscache
Display Name	DNS Client
Description	The DNS Client service (dnscache) sends Domain Name System (DNS) queries, caches query results, and registers the computer's full name on the network. This service is not stoppable.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k NetworkService -p
Service Execution Type	Own Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	nsi Afd

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Downloaded Maps Manager

Name	MapsBroker
Display Name	Downloaded Maps Manager
Description	Windows service for application access to downloaded maps. This service is started on-demand by application accessing downloaded maps. Disabling this service will prevent apps from accessing maps.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k NetworkService -p
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Embedded Mode

Name	embeddedmode
Display Name	Embedded Mode
Description	The Embedded Mode service enables scenarios related to Background Applications. Disabling this service will prevent Background Applications from being activated.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	BrokerInfrastructure

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Encrypting File System (EFS)

Name	EFS
Display Name	Encrypting File System (EFS)
Description	Provides the core file encryption technology used to store encrypted files on NTFS file system volumes. If this service is stopped or disabled, applications will be unable to access encrypted files.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\lsass.exe
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Enterprise App Management Service

Name	EntAppSvc
Display Name	Enterprise App Management Service
Description	Enables enterprise application management.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k appmodel -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Extensible Authentication Protocol

Name	EapHost
Display Name	Extensible Authentication Protocol
Description	The Extensible Authentication Protocol (EAP) service provides network authentication in such scenarios as 802.1x wired and wireless, VPN, and Network Access Protection (NAP). EAP also provides application programming interfaces (APIs) that are used by network access clients, including wireless and VPN clients, during the authentication process. If you disable this service, this computer is prevented from accessing networks that require EAP authentication.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS KeyIso

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Function Discovery Provider Host

Name	fdPHost
Display Name	Function Discovery Provider Host
Description	The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD providers supply network discovery services for the Simple Services Discovery Protocol (SSDP) and Web Services – Discovery (WS-D) protocol. Stopping or disabling the FDPHOST service will disable network discovery for these protocols when using FD. When this service is unavailable, network services using FD and relying on these discovery protocols will be unable to find network devices or resources.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs http

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Function Discovery Resource Publication

Name	FDResPub
Display Name	Function Discovery Resource Publication
Description	Publishes this computer and resources attached to this computer so they can be discovered over the network. If this service is stopped, network resources will no longer be published and they will not be discovered by other computers on the network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs http fdphost

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

GameInput Service

Name	GameInputSvc
Display Name	GameInput Service
Description	Enables keyboards, mice, gamepads, and other input devices to be used with the GameInput API.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\GameInputSvc.exe
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Geolocation Service

Name	lfsvc
Display Name	Geolocation Service
Description	This service monitors the current location of the system and manages geofences (a geographical location with associated events). If you turn off this service, applications will be unable to use or receive notifications for geolocation or geofences.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Google Chrome Elevation Service (GoogleChromeElevationService)

Name	GoogleChromeElevationService
Display Name	Google Chrome Elevation Service (GoogleChromeElevationService)
Description	Provides encryption services and a secure way for recovering Google Chrome if it gets out of date. If this service is disabled, Google Chrome may lose access to encrypted data, and Google Chrome may not be able recover itself.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Google\Chrome\Application\132.0.6834.197\elevation_service.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Google Updater Internal Service (GoogleUpdaterInternalService134.0.6985.0)

Name	GoogleUpdaterInternalService134.0.6985.0
Display Name	Google Updater Internal Service (GoogleUpdaterInternalService134.0.6985.0)
Description	Keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Google\GoogleUpdater\134.0.6985.0\updater.exe" --system --windows-service --service=update-internal
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Google Updater Service (GoogleUpdaterService134.0.6985.0)

Name	GoogleUpdaterService134.0.6985.0
Display Name	Google Updater Service (GoogleUpdaterService134.0.6985.0)
Description	Keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Google\GoogleUpdater\134.0.6985.0\updater.exe" --system --windows-service --service=update
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

GraphicsPerfSvc

Name	GraphicsPerfSvc
Display Name	GraphicsPerfSvc
Description	Graphics performance monitor service

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k GraphicsPerfSvcGroup
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	1440 minutes
Enable Actions for Stops with Errors	False

Group Policy Client

Name	gpsvc
Display Name	Group Policy Client
Description	The service is responsible for applying settings configured by administrators for the computer and users through the Group Policy component. If the service is disabled, the settings will not be applied and applications and components will not be manageable through Group Policy. Any components or applications that depend on the Group Policy component might not be functional if the service is disabled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k GPSvcGroup
Service Execution Type	Own Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RPCSS Mup

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Human Interface Device Service

Name	hidserv
Display Name	Human Interface Device Service
Description	Activates and maintains the use of hot buttons on keyboards, remote controls, and other multimedia devices. It is recommended that you keep this service running.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

HV Host Service

Name	HvHost
Display Name	HV Host Service
Description	Provides an interface for the Hyper-V hypervisor to provide per-partition performance counters to the host operating system.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	hvservice

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Hyper-V Data Exchange Service

Name	vmickvpexchange
Display Name	Hyper-V Data Exchange Service
Description	Provides a mechanism to exchange data between the virtual machine and the operating system running on the physical computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Hyper-V Guest Service Interface

Name	vmicguestinterface
Display Name	Hyper-V Guest Service Interface
Description	Provides an interface for the Hyper-V host to interact with specific services running inside the virtual machine.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Hyper-V Guest Shutdown Service

Name	vmicshutdown
Display Name	Hyper-V Guest Shutdown Service
Description	Provides a mechanism to shut down the operating system of this virtual machine from the management interfaces on the physical computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Hyper-V Heartbeat Service

Name	vmicheartbeat
Display Name	Hyper-V Heartbeat Service
Description	Monitors the state of this virtual machine by reporting a heartbeat at regular intervals. This service helps you identify running virtual machines that have stopped responding.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k ICService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Hyper-V PowerShell Direct Service

Name	vmicvmsession
Display Name	Hyper-V PowerShell Direct Service
Description	Provides a mechanism to manage virtual machine with PowerShell via VM session without a virtual network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Hyper-V Remote Desktop Virtualization Service

Name	vmicrdv
Display Name	Hyper-V Remote Desktop Virtualization Service
Description	Provides a platform for communication between the virtual machine and the operating system running on the physical computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k ICService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Hyper-V Time Synchronization Service

Name	vmictimesync
Display Name	Hyper-V Time Synchronization Service
Description	Synchronizes the system time of this virtual machine with the system time of the physical computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	VmGid

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Hyper-V Volume Shadow Copy Requestor

Name	vmicvss
Display Name	Hyper-V Volume Shadow Copy Requestor
Description	Coordinates the communications that are required to use Volume Shadow Copy Service to back up applications and data on this virtual machine from the operating system on the physical computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

IKE and AuthIP IPsec Keying Modules

Name	IKEEXT
Display Name	IKE and AuthIP IPsec Keying Modules
Description	The IKEEXT service hosts the Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are used for authentication and key exchange in Internet Protocol security (IPsec). Stopping or disabling the IKEEXT service will disable IKE and AuthIP key exchange with peer computers. IPsec is typically configured to use IKE or AuthIP; therefore, stopping or disabling the IKEEXT service might result in an IPsec failure and might compromise the security of the system. It is strongly recommended that you have the IKEEXT service running.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	BFE nsi

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Internet Connection Sharing (ICS)

Name	SharedAccess
Display Name	Internet Connection Sharing (ICS)
Description	Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	BFE

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Inventory and Compatibility Appraisal service

Name	InventorySvc
Display Name	Inventory and Compatibility Appraisal service
Description	This service performs background system inventory, compatibility appraisal, and maintenance used by numerous system components.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k InvSvcGroup -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

IP Helper

Name	iphlpsvc
Display Name	IP Helper
Description	Provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Teredo), and IP-HTTPS. If this service is stopped, the computer will not have the enhanced connectivity benefits that these technologies offer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k NetSvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSS tcpip nsi WinHttpAutoProxySvc

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

IPsec Policy Agent

Name	PolicyAgent
Display Name	IPsec Policy Agent
Description	Internet Protocol security (IPsec) supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. This service enforces IPsec policies created through the IP Security Policies snap-in or the command-line tool "netsh ipsec". If you stop this service, you may experience network connectivity issues if your policy requires that connections use IPsec. Also,remote management of Windows Defender Firewall is not available when this service is stopped.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k NetworkServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	Tcpip bfe

Log On

Account Name	NT Authority\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Services [J - R]

Displays the configuration of the Windows services on this machine

KDC Proxy Server service (KPS)

Name	KPSSVC
Display Name	KDC Proxy Server service (KPS)
Description	KDC Proxy Server service runs on edge servers to proxy Kerberos protocol messages to domain controllers on the corporate network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k KpsSvcGroup
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss http

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Kerberos Local Key Distribution Center

Name	LocalKdc
Display Name	Kerberos Local Key Distribution Center
Description	This service enables users to log on to the local machine using the Kerberos authentication protocol. If this service is stopped, users will be unable to log on to the local machine. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\lsass.exe
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

KtmRm for Distributed Transaction Coordinator

Name	KtmRm
Display Name	KtmRm for Distributed Transaction Coordinator
Description	Coordinates transactions between the Distributed Transaction Coordinator (MSDTC) and the Kernel Transaction Manager (KTM). If it is not needed, it is recommended that this service remain stopped. If it is needed, both MSDTC and KTM will start this service automatically. If this service is disabled, any MSDTC transaction interacting with a Kernel Resource Manager will fail and any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k NetworkServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS SamSS

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	True

Link-Layer Topology Discovery Mapper

Name	lltdsvc
Display Name	Link-Layer Topology Discovery Mapper
Description	Creates a Network Map, consisting of PC and device topology (connectivity) information, and metadata describing each PC and device. If this service is disabled, the Network Map will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss lltdio

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Local Session Manager

Name	LSM
Display Name	Local Session Manager
Description	Core Windows Service that manages local user sessions. Stopping or disabling this service will result in system instability.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcEptMapper DcomLaunch RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

LxpSvc

Name	LxpSvc
Display Name	LxpSvc
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

McpManagementService

Name	McpManagementService
Display Name	McpManagementService
Description	Universal Print Management Service

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k McpManagementServiceGroup
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Enable Actions for Stops with Errors	False

Microsoft Account Sign-in Assistant

Name	wlidsvc
Display Name	Microsoft Account Sign-in Assistant
Description	Enables user sign-in through Microsoft account identity services. If this service is stopped, users will not be able to logon to the computer with their Microsoft account.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Microsoft App-V Client

Name	AppVClient
Display Name	Microsoft App-V Client
Description	Manages App-V users and virtual applications

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\AppVClient.exe
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RpcSS netprofm AppvVfs AppVStrm

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Defender Antivirus Network Inspection Service

Name	WdNisSvc
Display Name	Microsoft Defender Antivirus Network Inspection Service
Description	Helps guard against intrusion attempts targeting known and newly discovered vulnerabilities in network protocols

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\NisSrv.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	WdNisDrv

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Microsoft Defender Antivirus Service

Name	WinDefend
Display Name	Microsoft Defender Antivirus Service
Description	Helps protect users from malware and other potentially unwanted software

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MsMpEng.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)

Name	MicrosoftEdgeElevationService
Display Name	Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)
Description	Keeps Microsoft Edge up to update. If this service is disabled, the application will not be kept up to date.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.59\elevation_service.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Edge Update Service (edgeupdate)

Name	edgeupdate
Display Name	Microsoft Edge Update Service (edgeupdate)
Description	Keeps your Microsoft software up to date. If this service is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Microsoft software using it.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Edge Update Service (edgeupdatem)

Name	edgeupdatem
Display Name	Microsoft Edge Update Service (edgeupdatem)
Description	Keeps your Microsoft software up to date. If this service is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Microsoft software using it.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /medsvc
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft iSCSI Initiator Service

Name	MSiSCSI
Display Name	Microsoft iSCSI Initiator Service
Description	Manages Internet SCSI (iSCSI) sessions from this computer to remote iSCSI target devices. If this service is stopped, this computer will not be able to login or access iSCSI targets. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	True

Microsoft Software Shadow Copy Provider

Name	swprv
Display Name	Microsoft Software Shadow Copy Provider
Description	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this service is stopped, software-based volume shadow copies cannot be managed. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k swprv
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Storage Spaces SMP

Name	smphost
Display Name	Microsoft Storage Spaces SMP
Description	Host service for the Microsoft Storage Spaces management provider. If this service is stopped or disabled, Storage Spaces cannot be managed.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k smphost
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	RPCSS

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Store Install Service

Name	InstallService
Display Name	Microsoft Store Install Service
Description	Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled then installations will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

NaturalAuthentication

Name	NaturalAuthentication
Display Name	NaturalAuthentication
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs ProfSvc Schedule

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Net.Tcp Port Sharing Service

Name	NetTcpPortSharing
Display Name	Net.Tcp Port Sharing Service
Description	Provides ability to share TCP ports over the net.tcp protocol.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Netlogon

Name	Netlogon
Display Name	Netlogon
Description	Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\lsass.exe
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	LanmanWorkstation

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Network Connection Broker

Name	NcbService
Display Name	Network Connection Broker
Description	Brokers connections that allow packaged Microsoft Store apps to receive notifications from the internet.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSS tcpip BrokerInfrastructure

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Network Connections

Name	Netman
Display Name	Network Connections
Description	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs nsi

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Network Connectivity Assistant

Name	NcaSvc
Display Name	Network Connectivity Assistant
Description	Provides DirectAccess status notification for UI components

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k NetSvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	BFE dnscache NSI iphlpsvc

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Network List Service

Name	netprofm
Display Name	Network List Service
Description	Identifies the networks to which the computer has connected, collects and stores properties for these networks, and notifies applications when these properties change.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netprofm -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	NSI RpcSs TcpIp

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Network Location Awareness

Name	NlaSvc
Display Name	Network Location Awareness
Description	Collects and stores configuration information for the network and notifies programs when this information is modified. If this service is stopped, configuration information might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netprofm -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Network Setup Service

Name	NetSetupSvc
Display Name	Network Setup Service
Description	The Network Setup Service manages the installation of network drivers and permits the configuration of low-level network settings. If this service is stopped, any driver installations that are in-progress may be cancelled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Network Store Interface Service

Name	nsi
Display Name	Network Store Interface Service
Description	This service delivers network notifications (e.g. interface addition/deleting etc) to user mode clients. Stopping this service will cause loss of network connectivity. If this service is disabled, any other services that explicitly depend on this service will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss nsiproxy

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

NgcCtnrSvc

Name	NgcCtnrSvc
Display Name	NgcCtnrSvc
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

NgcSvc

Name	NgcSvc
Display Name	NgcSvc
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Now Playing Session Manager Service_1c2dca

Name	NPSMSvc_1c2dca
Display Name	Now Playing Session Manager Service_1c2dca
Description	This service hosts the Now Playing Session Manager used for Media Scenarios

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Unknown
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Offline Files

Name	CscService
Display Name	Offline Files
Description	The Offline Files service performs maintenance activities on the Offline Files cache, responds to user logon and logoff events, implements the internals of the public API, and dispatches interesting events to those interested in Offline Files activities and changes in cache state.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

OpenSSH Authentication Agent

Name	ssh-agent
Display Name	OpenSSH Authentication Agent
Description	Agent to hold private keys used for public key authentication.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\OpenSSH\ssh-agent.exe
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

OpenSSH SSH Server

Name	sshd
Display Name	OpenSSH SSH Server
Description	SSH protocol based service to provide secure encrypted communications between two untrusted hosts over an insecure network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\OpenSSH\sshd.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Optimize drives

Name	defragsvc
Display Name	Optimize drives
Description	Helps the computer run more efficiently by optimizing files on storage drives.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k defragsvc
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	localSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

P9RdrService_1c2dca

Name	P9RdrService_1c2dca
Display Name	P9RdrService_1c2dca
Description	Enables trigger-starting plan9 file servers.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k P9RdrService -p
Service Execution Type	Unknown
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Payments and NFC/SE Manager

Name	SEMgrSvc
Display Name	Payments and NFC/SE Manager
Description	Manages payments and Near Field Communication (NFC) based secure elements.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Performance Counter DLL Host

Name	PerfHost
Display Name	Performance Counter DLL Host
Description	Enables remote users and 64-bit processes to query performance counters provided by 32-bit DLLs. If this service is stopped, only local users and 32-bit processes will be able to query performance counters provided by 32-bit DLLs.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\SysWow64\perfhost.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Performance Logs & Alerts

Name	pla
Display Name	Performance Logs & Alerts
Description	Performance Logs and Alerts Collects performance data from local or remote computers based on preconfigured schedule parameters, then writes the data to a log or triggers an alert. If this service is stopped, performance information will not be collected. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalServiceNoNetwork -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Plug and Play

Name	PlugPlay
Display Name	Plug and Play
Description	Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Portable Device Enumerator Service

Name	WPDBusEnum
Display Name	Portable Device Enumerator Service
Description	Enforces group policy for removable mass-storage devices. Enables applications such as Windows Media Player and Image Import Wizard to transfer and synchronize content using removable mass-storage devices.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Power

Name	Power
Display Name	Power
Description	Manages power policy and power policy notification delivery.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Restart the Computer
Subsequent Failure Action	Restart the Computer
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	1 minutes

Print Device Configuration Service

Name	PrintDeviceConfigurationService
Display Name	Print Device Configuration Service
Description	The Print Device Configuration Service manages the installation of IPP and UP printers. If this service is stopped, any printer installations that are in-progress may be canceled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Print Spooler

Name	Spooler
Display Name	Print Spooler
Description	This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't be able to print or see your printers.

Advanced

Allow Interaction With Desktop	True
Path Name	C:\WINDOWS\System32\spoolsv.exe
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RPCSS http

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Printer Extensions and Notifications

Name	PrintNotify
Display Name	Printer Extensions and Notifications
Description	This service opens custom printer dialog boxes and handles notifications from a remote print server or a printer. If you turn off this service, you won't be able to see printer extensions or notifications.

Advanced

Allow Interaction With Desktop	True
Path Name	C:\WINDOWS\system32\svchost.exe -k print
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

PrintScanBrokerService

Name	PrintScanBrokerService
Display Name	PrintScanBrokerService
Description	Provides support for secure privileged operations needed by low priv spooler.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

PrintWorkflow_1c2dca

Name	PrintWorkflowUserSvc_1c2dca
Display Name	PrintWorkflow_1c2dca
Description	Provides support for Print Workflow applications. If you turn off this service, you may not be able to print successfully.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k PrintWorkflow
Service Execution Type	Unknown
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Problem Reports Control Panel Support

Name	wercplsupport
Display Name	Problem Reports Control Panel Support
Description	This service provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports control panel.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	localSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Program Compatibility Assistant Service

Name	PcaSvc
Display Name	Program Compatibility Assistant Service
Description	This service provides support for the Program Compatibility Assistant (PCA). PCA monitors programs installed and run by the user and detects known compatibility problems. If this service is stopped, PCA will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Quality Windows Audio Video Experience

Name	QWAVE
Display Name	Quality Windows Audio Video Experience
Description	Quality Windows Audio Video Experience (qWave) is a networking platform for Audio Video (AV) streaming applications on IP home networks. qWave enhances AV streaming performance and reliability by ensuring network quality-of-service (QoS) for AV applications. It provides mechanisms for admission control, run time monitoring and enforcement, application feedback, and traffic prioritization.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss psched QWAVEdrv LLTDIO

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Radio Management Service

Name	RmSvc
Display Name	Radio Management Service
Description	Radio Management and Airplane Mode Service

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

ReFS Dedup Service

Name	refsdedupsvc
Display Name	ReFS Dedup Service
Description	ReFS data deduplication and compression service to track file changes and run scheduled optimization jobs.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\ReFsDedupSvc.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs schedule

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Remote Access Auto Connection Manager

Name	RasAuto
Display Name	Remote Access Auto Connection Manager
Description	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RasAcd

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Remote Access Connection Manager

Name	RasMan
Display Name	Remote Access Connection Manager
Description	Manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	SstpSvc DnsCache

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Remote Desktop Configuration

Name	SessionEnv
Display Name	Remote Desktop Configuration
Description	Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop Services and Remote Desktop related configuration and session maintenance activities that require SYSTEM context. These include per-session temporary folders, RD themes, and RD certificates.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS LanmanWorkstation

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Remote Desktop Services

Name	TermService
Display Name	Remote Desktop Services
Description	Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the checkboxes on the Remote tab of the System properties control panel item.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k termsvcs
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	NT Authority\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Remote Desktop Services UserMode Port Redirector

Name	UmRdpService
Display Name	Remote Desktop Services UserMode Port Redirector
Description	Allows the redirection of Printers/Drives/Ports for RDP connections

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	TermService RDPDR

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Remote Procedure Call (RPC)

Name	RpcSs
Display Name	Remote Procedure Call (RPC)
Description	The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activations requests, object exporter resolutions and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k rpcss -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcEptMapper DcomLaunch

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	1 minutes

Remote Procedure Call (RPC) Locator

Name	RpcLocator
Display Name	Remote Procedure Call (RPC) Locator
Description	In Windows 2003 and earlier versions of Windows, the Remote Procedure Call (RPC) Locator service manages the RPC name service database. In Windows Vista and later versions of Windows, this service does not provide any functionality and is present for application compatibility.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\locator.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Remote Registry

Name	RemoteRegistry
Display Name	Remote Registry
Description	Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k localService -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Resultant Set of Policy Provider

Name	RSoPProv
Display Name	Resultant Set of Policy Provider
Description	Provides a network service that processes requests to simulate application of Group Policy settings for a target user or computer in various situations and computes the Resultant Set of Policy settings.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\RSoPProv.exe
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Routing and Remote Access

Name	RemoteAccess
Display Name	Routing and Remote Access
Description	Offers routing services to businesses in local area and wide area network environments.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RpcSS Bfe RasMan Http

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

RPC Endpoint Mapper

Name	RpcEptMapper
Display Name	RPC Endpoint Mapper
Description	Resolves RPC interfaces identifiers to transport endpoints. If this service is stopped or disabled, programs using Remote Procedure Call (RPC) services will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k RPCSS -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Services [S - Z]

Displays the configuration of the Windows services on this machine

Secondary Logon

Name	seclogon
Display Name	Secondary Logon
Description	Enables starting processes under alternate credentials. If this service is stopped, this type of logon access will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Secure Socket Tunneling Protocol Service

Name	SstpSvc
Display Name	Secure Socket Tunneling Protocol Service
Description	Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Security Accounts Manager

Name	SamSs
Display Name	Security Accounts Manager
Description	The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\lsass.exe
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Sensor Data Service

Name	SensorDataService
Display Name	Sensor Data Service
Description	Delivers data from a variety of sensors

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\SensorDataService.exe
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Sensor Monitoring Service

Name	SensrSvc
Display Name	Sensor Monitoring Service
Description	Monitors various sensors in order to expose data and adapt to system and user state. If this service is stopped or disabled, the display brightness will not adapt to lighting conditions. Stopping this service may affect other system functionality and features as well.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Sensor Service

Name	SensorService
Display Name	Sensor Service
Description	A service for sensors that manages different sensors' functionality. Manages Simple Device Orientation (SDO) and History for sensors. Loads the SDO sensor that reports device orientation changes. If this service is stopped or disabled, the SDO sensor will not be loaded and so auto-rotation will not occur. History collection from Sensors will also be stopped.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Server

Name	LanmanServer
Display Name	Server
Description	Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k smbsvcs
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	SamSS Srv2

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Shared PC Account Manager

Name	shpamsvc
Display Name	Shared PC Account Manager
Description	Manages profiles and accounts on a SharedPC configured device

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RpcSs ProfSvc

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Shell Hardware Detection

Name	ShellHWDetection
Display Name	Shell Hardware Detection
Description	Provides notifications for AutoPlay hardware events.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Smart Card

Name	SCardSvr
Display Name	Smart Card
Description	Manages access to smart cards read by this computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Smart Card Device Enumeration Service

Name	ScDeviceEnum
Display Name	Smart Card Device Enumeration Service
Description	Creates software device nodes for all smart card readers accessible to a given session. If this service is disabled, WinRT APIs will not be able to enumerate smart card readers.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Smart Card Removal Policy

Name	SCPolicySvc
Display Name	Smart Card Removal Policy
Description	Allows the system to be configured to lock the user desktop upon smart card removal.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

SNMP Trap

Name	SNMPTrap
Display Name	SNMP Trap
Description	Receives trap messages generated by local or remote Simple Network Management Protocol (SNMP) agents and forwards the messages to SNMP management programs running on this computer. If this service is stopped, SNMP-based programs on this computer will not receive SNMP trap messages. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\snmptrap.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Software Protection

Name	sppsvc
Display Name	Software Protection
Description	Enables the download, installation and enforcement of digital licenses for Windows and Windows applications. If the service is disabled, the operating system and licensed applications may run in a notification mode. It is strongly recommended that you not disable the Software Protection service.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\sppsvc.exe
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Special Administration Console Helper

Name	sacsvr
Display Name	Special Administration Console Helper
Description	Allows administrators to remotely access a command prompt using Emergency Management Services.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Spot Verifier

Name	svsvc
Display Name	Spot Verifier
Description	Verifies potential file system corruptions.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

SQL Server (SQLEXPRESS)

Name	MSSQL$SQLEXPRESS
Display Name	SQL Server (SQLEXPRESS)
Description	Provides storage, processing and controlled access of data, and rapid transaction processing.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Microsoft SQL Server\MSSQL16.SQLEXPRESS\MSSQL\Binn\sqlservr.exe" -sSQLEXPRESS
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	KEYISO

Log On

Account Name	NT Service\MSSQL$SQLEXPRESS

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

SQL Server Agent (SQLEXPRESS)

Name	SQLAgent$SQLEXPRESS
Display Name	SQL Server Agent (SQLEXPRESS)
Description	Executes jobs, monitors SQL Server, fires alerts, and allows automation of some administrative tasks.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Microsoft SQL Server\MSSQL16.SQLEXPRESS\MSSQL\Binn\SQLAGENT.EXE" -i SQLEXPRESS
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	MSSQL$SQLEXPRESS

Log On

Account Name	NT AUTHORITY\NETWORKSERVICE

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

SQL Server Browser

Name	SQLBrowser
Display Name	SQL Server Browser
Description	Provides SQL Server connection information to client computers.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe"
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LOCALSERVICE

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

SQL Server CEIP service (SQLEXPRESS)

Name	SQLTELEMETRY$SQLEXPRESS
Display Name	SQL Server CEIP service (SQLEXPRESS)
Description	CEIP service for Sql server

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Microsoft SQL Server\MSSQL16.SQLEXPRESS\MSSQL\Binn\sqlceip.exe" -Service SQLEXPRESS
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	NT Service\SQLTELEMETRY$SQLEXPRESS

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

SQL Server VSS Writer

Name	SQLWriter
Display Name	SQL Server VSS Writer
Description	Provides the interface to backup/restore Microsoft SQL server through the Windows VSS infrastructure.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

SSDP Discovery

Name	SSDPSRV
Display Name	SSDP Discovery
Description	Discovers networked devices and services that use the SSDP discovery protocol, such as UPnP devices. Also announces SSDP devices and services running on the local computer. If this service is stopped, SSDP-based devices will not be discovered. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	HTTP NSI

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

State Repository Service

Name	StateRepository
Display Name	State Repository Service
Description	Provides required infrastructure support for the application model.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k appmodel -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Still Image Acquisition Events

Name	WiaRpc
Display Name	Still Image Acquisition Events
Description	Launches applications associated with still image acquisition events.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Storage Service

Name	StorSvc
Display Name	Storage Service
Description	Provides enabling services for storage settings and external storage expansion

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Storage Tiers Management

Name	TieringEngineService
Display Name	Storage Tiers Management
Description	Optimizes the placement of data in storage tiers on all tiered storage spaces in the system.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\TieringEngineService.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Sync Host_1c2dca

Name	OneSyncSvc_1c2dca
Display Name	Sync Host_1c2dca
Description	This service synchronizes mail, contacts, calendar and various other user data. Mail and other applications dependent on this functionality will not work properly when this service is not running.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

SysMain

Name	SysMain
Display Name	SysMain
Description	Maintains and improves system performance over time.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

System Event Notification Service

Name	SENS
Display Name	System Event Notification Service
Description	Monitors system events and notifies subscribers to COM+ Event System of these events.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	EventSystem

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

System Events Broker

Name	SystemEventsBroker
Display Name	System Events Broker
Description	Coordinates execution of background work for WinRT application. If this service is stopped or disabled, then background work might not be triggered.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcEptMapper RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Restart the Computer
Subsequent Failure Action	Restart the Computer
Reset Failure Count	1 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	2 minutes

System Guard Runtime Monitor Broker

Name	SgrmBroker
Display Name	System Guard Runtime Monitor Broker
Description	Monitors and attests to the integrity of the Windows platform.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\Sgrm\SgrmBroker.exe
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Task Scheduler

Name	Schedule
Display Name	Task Scheduler
Description	Enables a user to configure and schedule automated tasks on this computer. The service also hosts multiple Windows system-critical tasks. If this service is stopped or disabled, these tasks will not be run at their scheduled times. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RPCSS SystemEventsBroker

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Unknown
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

TCP/IP NetBIOS Helper

Name	lmhosts
Display Name	TCP/IP NetBIOS Helper
Description	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on the network, therefore enabling users to share files, print, and log on to the network. If this service is stopped, these functions might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	Afd

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Telephony

Name	tapisrv
Display Name	Telephony
Description	Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also running the service.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Text Input Management Service

Name	TextInputManagementService
Display Name	Text Input Management Service
Description	Enables text input, expressive input, touch keyboard, handwriting, and IMEs.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Themes

Name	Themes
Display Name	Themes
Description	Provides user experience theme management.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Time Broker

Name	TimeBrokerSvc
Display Name	Time Broker
Description	Coordinates execution of background work for WinRT application. If this service is stopped or disabled, then background work might not be triggered.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Udk User Service_1c2dca

Name	UdkUserSvc_1c2dca
Display Name	Udk User Service_1c2dca
Description	Shell components service

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k UdkSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Update Orchestrator Service

Name	UsoSvc
Display Name	Update Orchestrator Service
Description	Manages Windows Updates. If stopped, your devices will not be able to download and install the latest updates.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

UPnP Device Host

Name	upnphost
Display Name	UPnP Device Host
Description	Allows UPnP devices to be hosted on this computer. If this service is stopped, any hosted UPnP devices will stop functioning and no additional hosted devices can be added. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	SSDPSRV HTTP

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

User Access Logging Service

Name	UALSVC
Display Name	User Access Logging Service
Description	This service logs unique client access requests, in the form of IP addresses and user names, of installed products and roles on the local server. This information can be queried, via Powershell, by administrators needing to quantify client demand of server software for offline Client Access License (CAL) management. If the service is disabled, client requests will not be logged and will not be retrievable via Powershell queries. Stopping the service will not affect query of historical data (see supporting documentation for steps to delete historical data). The local system administrator must consult his, or her, Windows Server license terms to determine the number of CALs that are required for the server software to be appropriately licensed; use of the UAL service and data does not alter this obligation.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	WinMgmt

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

User Data Access_1c2dca

Name	UserDataSvc_1c2dca
Display Name	User Data Access_1c2dca
Description	Provides apps access to structured user data, including contact info, calendars, messages, and other content. If you stop or disable this service, apps that use this data might not work correctly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

User Data Storage_1c2dca

Name	UnistoreSvc_1c2dca
Display Name	User Data Storage_1c2dca
Description	Handles storage of structured user data, including contact info, calendars, messages, and other content. If you stop or disable this service, apps that use this data might not work correctly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

User Experience Virtualization Service

Name	UevAgentService
Display Name	User Experience Virtualization Service
Description	Provides support for application and OS settings roaming

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\AgentService.exe
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

User Manager

Name	UserManager
Display Name	User Manager
Description	User Manager provides the runtime components required for multi-user interaction. If this service is stopped, some applications may not operate correctly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs ProfSvc

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

User Profile Service

Name	ProfSvc
Display Name	User Profile Service
Description	This service is responsible for loading and unloading user profiles. If this service is stopped or disabled, users will no longer be able to successfully sign in or sign out, apps might have problems getting to users' data, and components registered to receive profile event notifications won't receive them.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k UserProfileService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Virtual Disk

Name	vds
Display Name	Virtual Disk
Description	Provides management services for disks, volumes, file systems, and storage arrays.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\vds.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

VMware Alias Manager and Ticket Service

Name	VGAuthService
Display Name	VMware Alias Manager and Ticket Service
Description	Alias Manager and Ticket Service

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

VMware Snapshot Provider

Name	vmvss
Display Name	VMware Snapshot Provider
Description	VMware Snapshot Provider

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\dllhost.exe /Processid:{978B6A3C-A0A6-4A05-BDF8-4FEB013E2016}
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

VMware SVGA Helper Service

Name	VM3DService
Display Name	VMware SVGA Helper Service
Description	Helps VMware SVGA driver by collecting and conveying user mode information

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\vm3dservice.exe
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

VMware Tools

Name	VMTools
Display Name	VMware Tools
Description	Provides support for synchronizing objects between the host and guest operating systems.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Volume Shadow Copy

Name	VSS
Display Name	Volume Shadow Copy
Description	Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\vssvc.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

W3C Logging Service

Name	w3logsvc
Display Name	W3C Logging Service
Description	Provides W3C logging for Internet Information Services (IIS). If this service is stopped, W3C logging configured by IIS will not work.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k apphost
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	HTTP

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

WaaSMedicSvc

Name	WaaSMedicSvc
Display Name	WaaSMedicSvc
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k wusvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

WalletService

Name	WalletService
Display Name	WalletService
Description	Hosts objects used by clients of the wallet

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k appmodel -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Warp JIT Service

Name	WarpJITSvc
Display Name	Warp JIT Service
Description	Enables JIT compilation support in d3d10warp.dll for processes in which code generation is disabled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Web Account Manager

Name	TokenBroker
Display Name	Web Account Manager
Description	This service is used by Web Account Manager to provide single-sign-on to apps and services.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	UserManager BrokerInfrastructure

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Web Management Service

Name	WMSVC
Display Name	Web Management Service
Description	The Web Management Service enables remote and delegated management capabilities for administrators to manage for the Web server, sites and applications present on this machine.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\inetsrv\wmsvc.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	HTTP

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Wi-Fi Direct Services Connection Manager Service

Name	WFDSConMgrSvc
Display Name	Wi-Fi Direct Services Connection Manager Service
Description	Manages connections to wireless services, including wireless display and docking.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Audio

Name	Audiosrv
Display Name	Windows Audio
Description	Manages audio for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	AudioEndpointBuilder RpcSs

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	3 minutes
Enable Actions for Stops with Errors	False

Windows Audio Endpoint Builder

Name	AudioEndpointBuilder
Display Name	Windows Audio Endpoint Builder
Description	Manages audio devices for the Windows Audio service. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Windows Biometric Service

Name	WbioSrvc
Display Name	Windows Biometric Service
Description	The Windows biometric service gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k WbioSvcGroup
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Camera Frame Server

Name	FrameServer
Display Name	Windows Camera Frame Server
Description	Enables multiple clients to access video frames from camera devices.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k Camera
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Camera Frame Server Monitor

Name	FrameServerMonitor
Display Name	Windows Camera Frame Server Monitor
Description	Monitors the health and state for the Windows Camera Frame Server service.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k CameraMonitor
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	3 minutes
Enable Actions for Stops with Errors	False

Windows Connect Now - Config Registrar

Name	wcncsvc
Display Name	Windows Connect Now - Config Registrar
Description	WCNCSVC hosts the Windows Connect Now Configuration which is Microsoft's Implementation of Wireless Protected Setup (WPS) protocol. This is used to configure Wireless LAN settings for an Access Point (AP) or a Wireless Device. The service is started programmatically as needed.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Windows Connection Manager

Name	Wcmsvc
Display Name	Windows Connection Manager
Description	Makes automatic connect and disconnect decisions based on the network connectivity options currently available to the PC and enables management of network connectivity based on Group Policy settings.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Wcmsvc
Service Execution Type	Own Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs NSI WinHttpAutoProxySvc

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Defender Advanced Threat Protection Service

Name	Sense
Display Name	Windows Defender Advanced Threat Protection Service
Description	Windows Defender Advanced Threat Protection service helps protect against advanced threats by monitoring and reporting security events that happen on the computer.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Defender Firewall

Name	mpssvc
Display Name	Windows Defender Firewall
Description	Windows Defender Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	mpsdrv bfe nsi

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Restart the Computer
Subsequent Failure Action	Restart the Computer
Reset Failure Count	1 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	1 minutes

Windows Encryption Provider Host Service

Name	WEPHOSTSVC
Display Name	Windows Encryption Provider Host Service
Description	Windows Encryption Provider Host Service brokers encryption related functionalities from 3rd Party Encryption Providers to processes that need to evaluate and apply EAS policies. Stopping this will compromise EAS compliancy checks that have been established by the connected Mail Accounts

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k WepHostSvcGroup
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Error Reporting Service

Name	WerSvc
Display Name	Windows Error Reporting Service
Description	Allows errors to be reported when programs stop working or responding and allows existing solutions to be delivered. Also allows logs to be generated for diagnostic and repair services. If this service is stopped, error reporting might not work correctly and results of diagnostic services and repairs might not be displayed.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k WerSvcGroup
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Event Collector

Name	Wecsvc
Display Name	Windows Event Collector
Description	This service manages persistent subscriptions to events from remote sources that support WS-Management protocol. This includes Windows Vista event logs, hardware and IPMI-enabled event sources. The service stores forwarded events in a local Event Log. If this service is stopped or disabled event subscriptions cannot be created and forwarded events cannot be accepted.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	HTTP Eventlog

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Event Log

Name	EventLog
Display Name	Windows Event Log
Description	This service manages events and event logs. It supports logging events, querying events, subscribing to events, archiving event logs, and managing event metadata. It can display events in both XML and plain text format. Stopping this service may compromise security and reliability of the system.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	True

Windows Font Cache Service

Name	FontCache
Display Name	Windows Font Cache Service
Description	Optimizes performance of applications by caching commonly used font data. Applications will start this service if it is not already running. It can be disabled, though doing so will degrade application performance.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Windows Image Acquisition (WIA)

Name	StiSvc
Display Name	Windows Image Acquisition (WIA)
Description	Provides image acquisition services for scanners and cameras

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k imgsvc
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Insider Service

Name	wisvc
Display Name	Windows Insider Service
Description	Provides infrastructure support for the Windows Insider Program. This service must remain enabled for the Windows Insider Program to work.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Installer

Name	msiserver
Display Name	Windows Installer
Description	Adds, modifies, and removes applications provided as a Windows Installer (*.msi, *.msp) package. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\msiexec.exe /V
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows License Manager Service

Name	LicenseManager
Display Name	Windows License Manager Service
Description	Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled then content acquired through the Microsoft Store will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	NT Authority\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Management Instrumentation

Name	Winmgmt
Display Name	Windows Management Instrumentation
Description	Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RPCSS

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Media Player Network Sharing Service

Name	WMPNetworkSvc
Display Name	Windows Media Player Network Sharing Service
Description	Shares Windows Media Player libraries to other networked players and media devices using Universal Plug and Play

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Windows Media Player\wmpnetwk.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	http WSearch

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Windows Modules Installer

Name	TrustedInstaller
Display Name	Windows Modules Installer
Description	Enables installation, modification, and removal of Windows updates and optional components. If this service is disabled, install or uninstall of Windows updates might fail for this computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\servicing\TrustedInstaller.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Process Activation Service

Name	WAS
Display Name	Windows Process Activation Service
Description	The Windows Process Activation Service (WAS) provides process activation, resource management and health management services for message-activated applications.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k iissvcs
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	RPCSS

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Windows Push Notifications System Service

Name	WpnService
Display Name	Windows Push Notifications System Service
Description	This service runs in session 0 and hosts the notification platform and connection provider which handles the connection between the device and WNS server.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	True

Windows Push Notifications User Service_1c2dca

Name	WpnUserService_1c2dca
Display Name	Windows Push Notifications User Service_1c2dca
Description	This service hosts Windows notification platform which provides support for local and push notifications. Supported notifications are tile, toast and raw.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Windows PushToInstall Service

Name	PushToInstall
Display Name	Windows PushToInstall Service
Description	Provides infrastructure support for the Microsoft Store. This service is started automatically and if disabled then remote installations will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Windows Remote Management (WS-Management)

Name	WinRM
Display Name	Windows Remote Management (WS-Management)
Description	Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The WinRM Service needs to be configured with a listener using winrm.cmd command line tool or through Group Policy in order for it to listen over the network. The WinRM service provides access to WMI data and enables event collection. Event collection and subscription to events require that the service is running. WinRM messages use HTTP and HTTPS as transports. The WinRM service does not depend on IIS but is preconfigured to share a port with IIS on the same machine. The WinRM service reserves the /wsman URL prefix. To prevent conflicts with IIS, administrators should ensure that any websites hosted on IIS do not use the /wsman URL prefix.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RPCSS HTTP NSI

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Search

Name	WSearch
Display Name	Windows Search
Description	Provides content indexing, property caching, and search results for files, e-mail, and other content.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\SearchIndexer.exe /Embedding
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RPCSS BrokerInfrastructure

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	True

Windows Security Service

Name	SecurityHealthService
Display Name	Windows Security Service
Description	Windows Security Service handles unified device protection and health information

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\SecurityHealthService.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Windows Time

Name	W32Time
Display Name	Windows Time
Description	Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalService
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Windows Update

Name	wuauserv
Display Name	Windows Update
Description	Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

WinHTTP Web Proxy Auto-Discovery Service

Name	WinHttpAutoProxySvc
Display Name	WinHTTP Web Proxy Auto-Discovery Service
Description	WinHTTP implements the client HTTP stack and provides developers with a Win32 API and COM Automation component for sending HTTP requests and receiving responses. In addition, WinHTTP provides support for auto-discovering a proxy configuration via its implementation of the Web Proxy Auto-Discovery (WPAD) protocol.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	Dhcp DNSCache

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1000 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Wired AutoConfig

Name	dot3svc
Display Name	Wired AutoConfig
Description	The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs Ndisuio Eaphost

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

WLAN AutoConfig

Name	WlanSvc
Display Name	WLAN AutoConfig
Description	The WLANSVC service provides the logic required to configure, discover, connect to, and disconnect from a wireless local area network (WLAN) as defined by IEEE 802.11 standards. It also contains the logic to turn your computer into a software access point so that other devices or computers can connect to your computer wirelessly using a WLAN adapter that can support this. Stopping or disabling the WLANSVC service will make all WLAN adapters on your computer inaccessible from the Windows networking UI. It is strongly recommended that you have the WLANSVC service running if your computer has a WLAN adapter.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k WlansvcGroup
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	nativewifip RpcSs Ndisuio

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

WManSvc

Name	WManSvc
Display Name	WManSvc
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

WMI Performance Adapter

Name	wmiApSrv
Display Name	WMI Performance Adapter
Description	Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\wbem\WmiApSrv.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	localSystem

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Work Folders

Name	workfolderssvc
Display Name	Work Folders
Description	This service syncs files with the Work Folders server, enabling you to use the files on any of the PCs and devices on which you've set up Work Folders.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs wsearch

Log On

Account Name	NT AUTHORITY\LocalService

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Workstation

Name	LanmanWorkstation
Display Name	Workstation
Description	Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\System32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	MRxSmb20 NSI Bowser

Log On

Account Name	NT AUTHORITY\NetworkService

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

World Wide Web Publishing Service

Name	W3SVC
Display Name	World Wide Web Publishing Service
Description	Provides Web connectivity and administration through the Internet Information Services Manager

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k iissvcs
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	WAS HTTP

Log On

Account Name	localSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

XblAuthManager

Name	XblAuthManager
Display Name	XblAuthManager
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs

Log On

Account Name	LocalSystem

Recovery

First Failure Action	Take No Action
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

XIA Configuration Scheduler

Name	XCSSchedulerService
Display Name	XIA Configuration Scheduler
Description	Schedules actions on the XIA Configuration Server.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Scheduler\CENTREL.XIA.Configuration.Server.Scheduler.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	W3SVC

Log On

Account Name	NT AUTHORITY\NETWORK SERVICE

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

XIA Configuration Service

Name	XIAConfigurationSvc
Display Name	XIA Configuration Service
Description	Accesses and documents network devices for the CENTREL Solutions - XIA Configuration Server

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	

Log On

Account Name	CONTOSO\sysadmin

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No Action
Subsequent Failure Action	Take No Action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Time

The Windows Time service, also known as W32Time, synchronizes the date on Windows computers. Time synchronization is critical for the proper operation of many Windows services and line-of-business applications.

Active Directory

Domain Role	Member Server

Service Information

Start Mode	Automatic (Trigger Start)
Service State	Running

Global Settings

MaxNegPhaseCorrection	4,294,967,295
MaxPosPhaseCorrection	4,294,967,295
VMIC Provider Status	Enabled

Client Settings

Enabled	True
Client Type	Domain Hierarchy (NT5DS)
Special Poll Interval	1,024

Server Settings

Enabled	False

Support Provisions

This section provides information about the support provisions associated with this item.

2 Support Provisions

Name	Relationship Type	Hours	Start Date	Expiry Date
Network Support	Technical Support	8am-5pm	Friday, February 14, 2025	Saturday, February 14, 2026
Hardware Warranty	Hardware Maintenance	9-5pm Mon-Fri	Friday, February 14, 2025	Saturday, February 14, 2026

Network Support

This section provides information about the support provisions associated with this item.

Relationship Information

Relationship Type	Technical Support

Support Provision Details

Support Hours	8am-5pm
Reference Number	53964
Self Service Web Site	http://www.contoso.com
Email Address	support@contoso.com
Telephone Number	+44 (0)1234 123456

Validity Period

Start Date	Friday, February 14, 2025
Expiry Date	Saturday, February 14, 2026

Hardware Warranty

This section provides information about the support provisions associated with this item.

Relationship Information

Relationship Type	Hardware Maintenance

Support Provision Details

Support Hours	9-5pm Mon-Fri
Reference Number	633673356
Self Service Web Site	http://www.hpwarranty.com/logcall.aspx
Email Address	support@hpwarranty.com
Telephone Number	+44 (0)1235 589123

Validity Period

Start Date	Friday, February 14, 2025
Expiry Date	Saturday, February 14, 2026

Version History

The version history displays the changes that have been made to the documentation of this item over time - either automatically when a change has been detected, or manually by users of the system.

12 versions

Version	Username	Date	Time	Description
1.11	CONTOSO\sysadmin	Friday, February 14, 2025	3:52 PM	Updated by XIA Configuration Client Data
1.10	CONTOSO\sysadmin	Friday, February 14, 2025	3:37 PM	Added item general information
1.09	CONTOSO\sysadmin	Friday, February 14, 2025	3:31 PM	Updated by XIA Configuration Client Data
1.08	CONTOSO\sysadmin	Friday, February 14, 2025	3:16 PM	Updated by XIA Configuration Client Data
1.07	CONTOSO\sysadmin	Friday, February 14, 2025	3:09 PM	Updated by XIA Configuration Client Data
1.06	CONTOSO\sysadmin	Friday, February 14, 2025	1:46 PM	Updated by XIA Configuration Client Data
1.05	CONTOSO\sysadmin	Friday, February 14, 2025	1:40 PM	Updated by XIA Configuration Client Data
1.04	CONTOSO\sysadmin	Friday, February 14, 2025	12:25 PM	Updated by XIA Configuration Client Data
1.03	CONTOSO\sysadmin	Friday, February 14, 2025	12:15 PM	Updated by XIA Configuration Client Data
1.02	CONTOSO\sysadmin	Friday, February 14, 2025	12:13 PM	Updated by XIA Configuration Client Data
1.01	CONTOSO\sysadmin	Friday, January 3, 2025	5:18 PM	Updated by XIA Configuration Client Data
1.00	CONTOSO\sysadmin	Friday, January 3, 2025	5:18 PM	Item created.