

Windows Server Documentation

CSDEMO-DC01

Company Confidential

Document Properties

Author	CSDEMO\Administrator
Product	XIA Configuration Express [18.1.6.0]
Date	21 September 2026 11:55:25
Version	1.00



Table of Contents

Management Summary.....	3
General Information.....	5
Compliance Benchmarks.....	6
Windows Security Benchmark [6.0.0.0].....	7
Hardware.....	30
BIOS.....	31
Devices.....	32
Disk Drives.....	36
[0] VMware, VMware Virtual S SCSI Disk Device.....	37
[1] VMware Virtual NVMe Disk.....	39
Disk Volumes.....	41
C: (System).....	42
D: (Data).....	44
EFI System Partition (b0bbb371-44e3-439e-a4eb-046083980853).....	46
Recovery Partition (233d1a52-6c14-4f2b-a918-5cfb8ff8ec94).....	47
Optical Drives.....	48
Physical Memory.....	49
Physical Memory 0.....	50
Printers.....	51
Microsoft Print to PDF.....	52
Processors.....	53
11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz.....	54
11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz.....	55
Trusted Platform Module (TPM).....	56
Video Controllers.....	57
VMware SVGA 3D.....	58
Networking.....	59
Failover Clustering.....	60
Hosts File.....	61
IPv4 Routing Table.....	63
Network Adapters.....	64
Ethernet0.....	65
Network Load Balancing.....	68
Remote Assistance.....	69
Remote Desktop.....	70
Shares.....	71
ADMIN\$.....	72
C\$.....	73

D\$.....	74
IPC\$.....	75
NETLOGON.....	76
Public.....	77
SYSVOL.....	78
SNMP Configuration.....	80
Security.....	81
Advanced Audit Policy.....	82
Audit Policy.....	85
Certificates.....	86
Personal.....	87
157f8a9e-052c-4fc2-8b9f-11e8ccc55e96.....	88
WindowsAdminCenterSelfSigned.....	89
Local Account Policies.....	90
Microsoft Defender.....	91
Security Options.....	92
User Rights Assignment.....	104
Windows Firewall.....	108
Domain Profile.....	109
Private Profile.....	110
Public Profile.....	111
Inbound Rules.....	112
Outbound Rules.....	121
Windows Patches.....	127
Windows Update Configuration.....	128
Windows Update History.....	129
Software.....	137
.NET Framework.....	138
Environment Variables.....	139
Event Logs.....	141
Active Directory Web Services.....	142
Application.....	144
DFS Replication.....	146
Directory Service.....	148
DNS Server.....	150
ECMA2Host.....	152
Forwarded Events.....	154
Hardware Events.....	156
Key Management Service.....	158
Security.....	160
Setup.....	162
System.....	164

Windows PowerShell.....	166
WindowsAdminCenter.....	168
Installed Software.....	170
Internet Settings.....	171
ODBC Configuration.....	172
ODBC Drivers.....	173
ODBC Data Sources.....	174
Operating System.....	175
PowerShell Settings.....	177
Registry.....	178
Roles and Features.....	179
Task Scheduler Library.....	188
azcmagent.....	189
CreateExplorerShellUnelevatedTask.....	191
GoogleUpdaterTaskSystem152.0.7933.0{560858BF-9381-4356-A4A1-F6958A00D7B2}.....	193
MicrosoftEdgeUpdateTaskMachineCore{0180DB29-C278-4BBC-BD83-2AD720678EF4}.....	195
MicrosoftEdgeUpdateTaskMachineUA{0788BB83-9448-4452-B945-D7FABFF6FCF7}.....	197
WindowsAdminCenterUpdater.....	199
Startup Commands.....	201
Windows Remote Management (WinRM).....	202
Windows Services.....	204
Windows Time.....	217



Management Summary

Provides a management summary for this machine.

Operating System

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



Windows Server 2025
Datacenter

Naming and Role

Domain	centrelsolutionsdemo.int
Domain Role	Domain Controller (PDC emulator)
NetBIOS Name	CSDEMO-DC01
Fully Qualified Domain Name	csdemo-dc01.centrelsolutionsdemo.int

Hardware Information

Serial Number	VMware-56 4d 4f 0e f3 9a ef 95-ed 03 ca f3 02 f9 14 fe
Manufacturer	VMware, Inc.
Model	VMware20,1
Asset Tag	

Networking Information

Network Adapters	5 Network Adapters
IPv4 Addresses	192.168.176.132/24
IPv6 Addresses	fe80::7900:9a83:7941:7a91%5/0.0.0.64

Remote Desktop Settings

Allow Connections	False
-------------------	-------

2 Server Functions

Name	Enabled	Active	Instance Identifier
 DNS Server	True	True	
 Domain Controller	True	True	



General Information

Provides general information for this item.

General Information

Name	CSDEMO-DC01
Description	Demonstration domain controller.
Primary Owner Name	
Primary Owner Contact	



Compliance Benchmarks

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



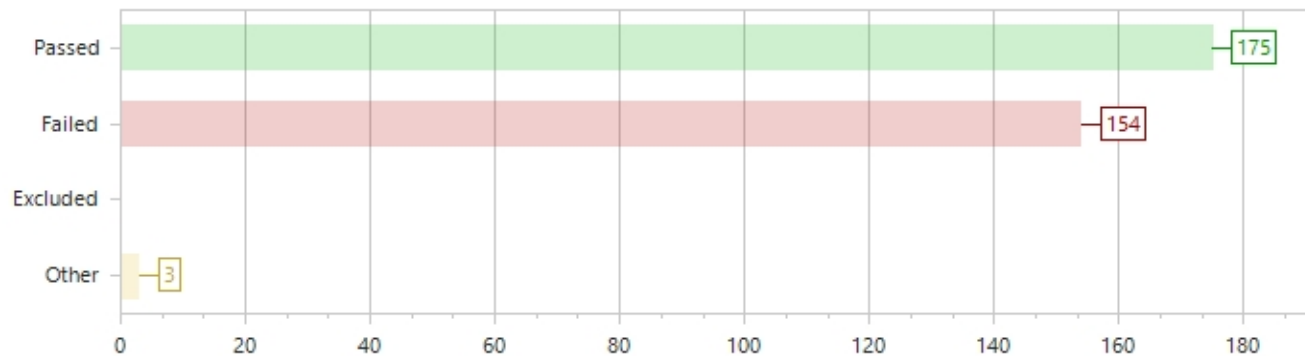
1 Compliance Benchmarks

Name	Version	Passed	Failed	Other
 Windows Security Benchmark	6.0.0.0	175	154	3



Windows Security Benchmark [6.0.0.0]

The Windows Security Benchmark evaluates the security configuration of Windows operating systems, including both physical and virtual servers and workstations. It provides a consistent baseline for assessing and comparing security related policies, audit controls, account settings, and system configuration. The benchmark automatically adapts to the role of each machine - workstation, server, or domain controller to ensure accurate and relevant compliance results across diverse Windows environments.



332 Benchmark Results

Ref.	Result	Title	Configured Value
------	--------	-------	------------------

Section 1: Password Policy

✓	1.01	Passed	Set "Enforce password history" to remember at least 24 passwords	24
✓	1.02	Passed	Set "Maximum password age" to 60 days or less	42 days
✓	1.03	Passed	Set "Minimum password age" to at least 1 day(s)	1 days
✗	1.04	Failed	Set "Minimum password length" to 14 or more characters	7
✓	1.05	Passed	Set "Password must meet complexity requirements" to "Enabled"	Enabled

✓	1.06	Passed	Set "Store passwords using reversible encryption" to "Disabled"	False
✗	1.07	Failed	Set "Relax minimum password length limits" to "Enabled" on supported operating systems	Not Configured

Section 2: Account Lockout Policy

✗	2.01	Failed	Set the "Account lockout duration" to 30 minutes or longer	Not Applicable
✗	2.02	Failed	Set the "Account lockout threshold" to greater than 4 and less than 10	0
✗	2.03	Failed	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	Failed	Set "Allow Basic Authentication" to "False" for the WinRM Client	True
✗	3.02	Failed	Set "Allow Digest Authentication" to "False" for the WinRM Client	True
✓	3.03	Passed	Set "Allow Unencrypted Traffic" to "False" for the WinRM Client	False
✓	3.04	Passed	Set "Allow Basic Authentication" to "False" for the WinRM Service	False
✓	3.05	Passed	Set "Allow Unencrypted Traffic" to "False" for the WinRM Service	False
✗	3.06	Failed	Set "Disallow Storing RunAs Credentials" to "True" for the WinRM Service	False
✓	3.07	Passed	Set "Allow Remote Shell Access" to "True" for the Windows Remote Shell	True

Section 5: Server Functions

✗	5.01	Failed	Limit the number of server functions to one per server	DNS Server Domain Controller
---	------	--------	--	---------------------------------

Section 6: Remote Desktop Settings

✓	6.01	Passed	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	Passed	Set "Disable COM Port Redirection" to "True"	Don't allow remote connections
✓	6.03	Passed	Set "Disable Drive Redirection" to "True"	Don't allow remote connections

✓	6.04	Passed	Set "Disable LPT Port Redirection" to "True"	Don't allow remote connections
✓	6.05	Passed	Set "Disable Plug and Play Device" to "True"	Don't allow remote connections
✓	6.06	Passed	Set "Always Prompt For Password" to "True"	Don't allow remote connections
✓	6.07	Passed	Set "Security Layer" to "SSL"	Don't allow remote connections
✓	6.08	Passed	Set "Minimum Encryption Level" to "High"	Don't allow remote connections
✓	6.09	Passed	Set "Single Session Restriction" to "True"	Don't allow remote connections
✓	6.10	Passed	Set "Use Temporary Folders Per Session" to "True"	Don't allow remote connections
✓	6.11	Passed	Set "Delete Temporary Folders On Exit" to "True"	Don't allow remote connections
✓	6.12	Passed	Set "Require Secure RPC Communication" to "True"	Don't allow remote connections

Section 7: Audit Settings

✓	7.01	Passed	Set "Audit: Audit the access of global system objects" to "Disabled"	Disabled
✓	7.02	Passed	Set "Audit: Audit the use of Backup and Restore privilege" to "Disabled"	Disabled
✗	7.03	Failed	Set "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to "Enabled"	Not Defined
✗	7.04	Failed	Set the "Audit Credential Validation" advanced audit policy to "Success and Failure"	Success
✗	7.05	Failed	Set the "Audit Kerberos Authentication Service" advanced audit policy to "Success and Failure"	Success
✗	7.06	Failed	Set the "Audit Kerberos Service Ticket Operations" advanced audit policy to "Success and Failure"	Success
✗	7.07	Failed	Set the "Audit Other Account Logon Events" advanced audit policy to "Success and Failure"	None
✓	7.08	Passed	Set the "Audit Application Group Management" advanced audit policy to "None"	None
✗	7.09	Failed	Set the "Audit Computer Account Management" advanced audit policy to "Success and Failure"	Success
✓	7.10	Passed	Set the "Audit Distribution Group Management" advanced audit policy to "None"	None
✗	7.11	Failed	Set the "Audit Other Account Management Events" advanced audit policy to "Success and Failure"	None

✗ 7.12	Failed	Set the "Audit Security Group Management" advanced audit policy to "Success and Failure"	Success
✗ 7.13	Failed	Set the "Audit User Account Management" advanced audit policy to "Success and Failure"	Success
✗ 7.14	Failed	Set the "Audit DPAPI Activity" advanced audit policy to "Success and Failure"	None
✓ 7.15	Passed	Set the "Audit PNP Activity" advanced audit policy to "Any"	None
✗ 7.16	Failed	Set the "Audit Process Creation" advanced audit policy to "Success and Failure"	None
✓ 7.17	Passed	Set the "Audit Process Termination" advanced audit policy to "None"	None
✓ 7.18	Passed	Set the "Audit RPC Events" advanced audit policy to "None"	None
✓ 7.19	Passed	Set the "Audit Detailed Directory Service Replication" advanced audit policy to "None" on domain controllers	None
✓ 7.20	Passed	Set the "Audit Directory Service Access" advanced audit policy to "None" on domain controllers	Success
✓ 7.21	Passed	Set the "Audit Directory Service Changes" advanced audit policy to "None" on domain controllers	None
✓ 7.22	Passed	Set the "Audit Directory Service Replication" advanced audit policy to "None" on domain controllers	None
✓ 7.23	Passed	Set the "Audit Account Lockout" advanced audit policy to "Success"	Success
✗ 7.24	Failed	Set the "Audit Group Membership" advanced audit policy to "Success"	None
✓ 7.25	Passed	Set the "Audit IPsec Extended Mode" advanced audit policy to "None"	None
✓ 7.26	Passed	Set the "Audit IPsec Main Mode" advanced audit policy to "None"	None
✓ 7.27	Passed	Set the "Audit IPsec Quick Mode" advanced audit policy to "None"	None
✓ 7.28	Passed	Set the "Audit Logoff" advanced audit policy to "Success"	Success
✓ 7.29	Passed	Set the "Audit Logon" advanced audit policy to "Success and Failure"	Success and Failure
✓ 7.30	Passed	Set the "Audit Network Policy Server" advanced audit policy to "None"	Success and Failure
✓ 7.31	Passed	Set the "Audit Other Logon/Logoff Events" advanced audit policy to "None"	None
✗ 7.32	Failed	Set the "Audit Special Logon" advanced audit policy to "Success and Failure"	Success

✓ 7.33	Passed	Set the "Audit User/Device Claims" advanced audit policy to "None"	None
✓ 7.34	Passed	Set the "Audit Application Generated" advanced audit policy to "None"	None
✓ 7.35	Passed	Set the "Audit Central Access Policy Staging" advanced audit policy to "None"	None
✓ 7.36	Passed	Set the "Audit Certification Services" advanced audit policy to "None"	None
✓ 7.37	Passed	Set the "Audit Detailed File Share" advanced audit policy to "None"	None
✓ 7.38	Passed	Set the "Audit File Share" advanced audit policy to "None"	None
✓ 7.39	Passed	Set the "Audit File System" advanced audit policy to "None"	None
✓ 7.40	Passed	Set the "Audit Filtering Platform Connection" advanced audit policy to "None"	None
✓ 7.41	Passed	Set the "Audit Filtering Platform Packet Drop" advanced audit policy to "None"	None
✓ 7.42	Passed	Set the "Audit Handle Manipulation" advanced audit policy to "None"	None
✓ 7.43	Passed	Set the "Audit Kernel Object" advanced audit policy to "None"	None
✓ 7.44	Passed	Set the "Audit Other Object Access Events" advanced audit policy to "None"	None
✓ 7.45	Passed	Set the "Audit Registry" advanced audit policy to "None"	None
✓ 7.46	Passed	Set the "Audit Removable Storage" advanced audit policy to "None"	None
✓ 7.47	Passed	Set the "Audit SAM" advanced audit policy to "None"	None
✗ 7.48	Failed	Set the "Audit Audit Policy Change" advanced audit policy to "Success and Failure"	Success
✗ 7.49	Failed	Set the "Audit Authentication Policy Change" advanced audit policy to "Success and Failure"	Success
✓ 7.50	Passed	Set the "Audit Authorization Policy Change" advanced audit policy to "None"	None
✓ 7.51	Passed	Set the "Audit Filtering Platform Policy Change" advanced audit policy to "None"	None
✗ 7.52	Failed	Set the "Audit MPSSVC Rule-Level Policy Change" advanced audit policy to "Success"	None
✓ 7.53	Passed	Set the "Audit Other Policy Change Events" advanced audit policy to "None"	None

✓ 7.54	Passed	Set the "Audit Non Sensitive Privilege Use" advanced audit policy to "None"	None
✓ 7.55	Passed	Set the "Audit Other Privilege Use Events" advanced audit policy to "None"	None
✓ 7.56	Passed	Set the "Audit Sensitive Privilege Use" advanced audit policy to "None"	None
✗ 7.57	Failed	Set the "Audit IPsec Driver" advanced audit policy to "Success and Failure"	None
✓ 7.58	Passed	Set the "Audit Other System Events" advanced audit policy to "None"	Success and Failure
✗ 7.59	Failed	Set the "Audit Security State Change" advanced audit policy to "Success and Failure"	Success
✗ 7.60	Failed	Set the "Audit Security System Extension" advanced audit policy to "Success and Failure"	None
✓ 7.61	Passed	Set the "Audit System Integrity" advanced audit policy to "Success and Failure"	Success and Failure

Section 8: Windows Update

✓ 8.01	Passed	Enable Windows Update to receive updates	Download updates but let me choose whether to install them
✗ 8.02	Failed	Configure Windows Update to use Windows Server Update Services (WSUS)	

Section 9: Windows Time

✓ 9.01	Passed	Enable the Windows Time client on all machines	True
✗ 9.02	Failed	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	Passed	Enable the NTP server for domain controllers, and disable for all other servers and workstations	True

Section 10: SNMP

✓ 10.01	Passed	If SNMP is enabled, ensure that no "public" or "private" SNMP community strings are configured	Not Installed
✓ 10.02	Passed	If SNMP is enabled, ensure that no writable SNMP community strings are configured	Not Installed

Section 11: Deprecated Components and Protocols

✓ 11.01	Passed	Ensure that Server Message Block (SMB) version 1 is disabled for the server service	Server Feature Disabled
---------	--------	---	-------------------------

✓	11.02	Passed	Ensure that Server Message Block (SMB) version 1 is disabled for the client	Disabled
---	-------	--------	---	----------

Section 12: Windows Event Log

✗	12.01	Failed	Set the maximum size of the Application event log to 40,960 KB or greater	20,480 KB
✓	12.02	Passed	Set the maximum size of the Security event log to 81,920 KB or greater	131,072 KB
✗	12.03	Failed	Set the maximum size of the Setup event log to 20,480 KB or greater	1,028 KB
✓	12.04	Passed	Set the maximum size of the System event log to 20,480 KB or greater	20,480 KB
✓	12.05	Passed	Set the retention policy of the Application event log to 'Overwrite events as needed'	Overwrite events as needed
✓	12.06	Passed	Set the retention policy of the Security event log to 'Overwrite events as needed'	Overwrite events as needed
✓	12.07	Passed	Set the retention policy of the Setup event log to 'Overwrite events as needed'	Overwrite events as needed
✓	12.08	Passed	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	Passed	Set the "Access Credential Manager as a trusted caller" user right to [Empty]	
✗	13.02	Failed	Set the "Access this computer from the network" user right to include only [ENTERPRISE_DOMAIN_CONTROLLERS] BUILTIN\Administrators NT AUTHORITY\Authenticated Users	BUILTIN\Administrators BUILTIN\Pre-Windows 2000 Compatible Access Everyone NT AUTHORITY\Authenticated Users NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
✓	13.03	Passed	Set the "Act as part of the operating system" user right to [Empty]	
✗	13.04	Failed	Set the "Add workstations to domain" user right to include only BUILTIN\Administrators on domain controllers	NT AUTHORITY\Authenticated Users
✓	13.05	Passed	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%	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE

		NT SERVICE\SQLAgent% NT SERVICE\SQLSERVERAGENT	
❌ 13.06	Failed	Set the "Allow log on locally" user right to include only BUILTIN\Account Operators BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Print Operators BUILTIN\Server Operators	BUILTIN\Account Operators BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Print Operators BUILTIN\Server Operators NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
✅ 13.07	Passed	Set the "Allow log on through Remote Desktop Services" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✅ 13.08	Passed	Set the "Back up files and directories" user right to include only BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators
✅ 13.09	Passed	Set the "Bypass traverse checking" user right to [Any Value]	BUILTIN\Administrators BUILTIN\Pre-Windows 2000 Compatible Access Everyone NT AUTHORITY\Authenticated Users NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE RESTRICTED SERVICES\PrintSpoolerService
✅ 13.10	Passed	Set the "Change the system time" user right to include only BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE	BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE
✅ 13.11	Passed	Set the "Change the time zone" user right to [Any Value]	BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE
✅ 13.12	Passed	Set the "Create a pagefile" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✅ 13.13	Passed	Set the "Create a token object" user right to [Empty]	
✅ 13.14	Passed	Set the "Create global objects" user right to include only	BUILTIN\Administrators

		BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE
✓ 13.15	Passed	Set the "Create permanent shared objects" user right to [Empty]	
✓ 13.16	Passed	Set the "Create symbolic links" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✓ 13.17	Passed	Set the "Debug programs" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✗ 13.18	Failed	Set the "Deny access to this computer from the network" user right to must include BUILTIN\Guests	
✗ 13.19	Failed	Set the "Deny log on as a batch job" user right to must include BUILTIN\Guests	
✗ 13.20	Failed	Set the "Deny log on as a service" user right to must include BUILTIN\Guests	
✗ 13.21	Failed	Set the "Deny log on locally" user right to must include BUILTIN\Guests	
✗ 13.22	Failed	Set the "Deny log on through Remote Desktop Services" user right to must include BUILTIN\Guests	
✓ 13.23	Passed	Set the "Enable computer and user accounts to be trusted for delegation" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✗ 13.24	Failed	Set the "Force shutdown from a remote system" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Server Operators
✗ 13.25	Failed	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	NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE RESTRICTED SERVICES\PrintSpoolerService
✗ 13.26	Failed	Set the "Impersonate a client after authentication" user right to include only	BUILTIN\Administrators

		BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE RESTRICTED SERVICES\PrintSpoolerService
✓ 13.27	Passed	Set the "Increase a process working set" user right to include only BUILTIN\Users S-1-5-32-583 Window Manager\Window Manager Group	BUILTIN\Users
✓ 13.28	Passed	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	Failed	Set the "Load and unload device drivers" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Print Operators
✓ 13.30	Passed	Set the "Lock pages in memory" user right to [Empty]	
✓ 13.31	Passed	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\Performance Log Users
✗ 13.32	Failed	Set the "Log on as a service" user right to include only IIS APPPOOL\% NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	CSDemo\Administrator CSDemo\pGMSA_c2ca7496\$ CSDemo\XiaClient NT SERVICE\ALL SERVICES NT SERVICE\himds RESTRICTED SERVICES\ALL RESTRICTED SERVICES
✗ 13.33	Failed	Set the "Manage auditing and security log" user right to include only BUILTIN\Administrators	BUILTIN\Administrators CSDemo\Exchange Servers
✓ 13.34	Passed	Set the "Modify an object label" user right to [Empty]	
✓ 13.35	Passed	Set the "Modify firmware environment values" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
ⓘ 13.36	Unknown	Set the "Obtain an impersonation token for another user in the same session" user right to include only	Unknown

		BUILTIN\Administrators	
✓ 13.37	Passed	Set the "Perform volume maintenance tasks" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✓ 13.38	Passed	Set the "Profile single process" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✓ 13.39	Passed	Set the "Profile system performance" user right to include only BUILTIN\Administrators NT SERVICE\WdiServiceHost	BUILTIN\Administrators NT SERVICE\WdiServiceHost
✓ 13.40	Passed	Set the "Remove computer from docking station" user right to [Any Value]	BUILTIN\Administrators
✓ 13.41	Passed	Set the "Replace a process level token" user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE
✗ 13.42	Failed	Set the "Restore files and directories" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators
✗ 13.43	Failed	Set the "Shut down the system" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Print Operators BUILTIN\Server Operators
✓ 13.44	Passed	Set the "Synchronize directory service data" user right to [Empty]	
✓ 13.45	Passed	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	Passed	Set the Windows Firewall domain profile firewall state to "On (recommended)"	On (recommended)
✓ 14.02	Passed	Set the Windows Firewall domain profile default inbound action to "Block (default)"	Block (default)
✓ 14.03	Passed	Set the Windows Firewall domain profile default outbound action to "Allow (default)"	Allow (default)

✓	14.04	Passed	Set the Windows Firewall domain profile display a notification setting to "No"	No
✓	14.05	Passed	Set the Windows Firewall domain profile excluded network interfaces to none	
✗	14.06	Failed	Set the Windows Firewall domain profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\DomainProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
✗	14.07	Failed	Set the Windows Firewall domain profile log file size limit to 16,384 KB or greater	4,096 KB
✗	14.08	Failed	Set the Windows Firewall domain profile log dropped packets setting to "Yes"	No
✗	14.09	Failed	Set the Windows Firewall domain profile log successful connections setting to "Yes"	No

Section 15: Windows Firewall Private Profile

✓	15.01	Passed	Set the Windows Firewall private profile firewall state to "On (recommended)"	On (recommended)
✓	15.02	Passed	Set the Windows Firewall private profile default inbound action to "Block (default)"	Block (default)
✓	15.03	Passed	Set the Windows Firewall private profile default outbound action to "Allow (default)"	Allow (default)
✓	15.04	Passed	Set the Windows Firewall private profile display a notification setting to "No"	No
✓	15.05	Passed	Set the Windows Firewall private profile excluded network interfaces to none	
✗	15.06	Failed	Set the Windows Firewall private profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PrivateProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
✗	15.07	Failed	Set the Windows Firewall private profile log file size limit to 16,384 KB or greater	4,096 KB
✗	15.08	Failed	Set the Windows Firewall private profile log dropped packets setting to "Yes"	No
✗	15.09	Failed	Set the Windows Firewall private profile log successful connections setting to "Yes"	No

Section 16: Windows Firewall Public Profile

✓	16.01	Passed	Set the Windows Firewall public profile firewall state to "On (recommended)"	On (recommended)
✓	16.02	Passed	Set the Windows Firewall public profile default inbound action to "Block (default)"	Block (default)
✓	16.03	Passed	Set the Windows Firewall public profile default outbound action to "Allow (default)"	Allow (default)
✓	16.04	Passed	Set the Windows Firewall public profile display a notification setting to "No"	No

✓	16.05	Passed	Set the Windows Firewall public profile excluded network interfaces to none	
✗	16.06	Failed	Set the Windows Firewall public profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PublicProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
✗	16.07	Failed	Set the Windows Firewall public profile log file size limit to 16,384 KB or greater	4,096 KB
✗	16.08	Failed	Set the Windows Firewall public profile log dropped packets setting to "Yes"	No
✗	16.09	Failed	Set the Windows Firewall public profile log successful connections setting to "Yes"	No

Section 17: Security Options (General)

✗	17.01	Failed	Set the "App Runtime: Allow Microsoft accounts to be optional" security option to "Enabled"	Not Defined
✗	17.02	Failed	Set the "Biometrics: Configure enhanced anti-spoofing" security option to "Enabled"	Not Defined
✗	17.03	Failed	Set the "Cloud Content: Turn off Microsoft consumer experiences" security option to "Enabled"	Not Defined
✗	17.04	Failed	Set the "Connect: Require pin for pairing" security option to "First Time" or "Always"	Not Defined
✗	17.05	Failed	Set the "OneDrive: Prevent the usage of OneDrive for file storage" security option to "Enabled"	Not Defined
✗	17.06	Failed	Set the "Regional and Language Options: Allow users to enable online speech recognition services" security option to "Disabled"	Not Defined
✗	17.07	Failed	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	Failed	Set the "Accounts: Block Microsoft accounts" security option to "Users can't add or log on with Microsoft accounts"	Not Defined
✓	18.02	Passed	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	Passed	Set the "Audit Process Creation: Include command line in process creation events" security option to "Disabled" or "Not Defined"	Not Defined
✓	19.02	Passed	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	Failed	Set the "Credential User Interface: Do not display the password reveal button" security option to "Enabled"	Not Defined
❌	20.02	Failed	Set the "Credential User Interface: Enumerate administrator accounts on elevation" security option to "Disabled"	Not Defined

Section 21: Security Options (Credentials Delegation)

❌	21.01	Failed	Set the "Credentials Delegation: Encryption Oracle Remediation" security option to "Force Updated Clients"	Not Defined
❌	21.02	Failed	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	Failed	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	Failed	Set the "Data Collection and Preview Builds: Do not show feedback notifications" security option to "Enabled"	Not Defined
❌	22.04	Failed	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	Failed	Set the "Devices: Allowed to format and eject removable media" security option to "Administrators"	Not Defined
✅	23.02	Passed	Set the "Devices: Prevent users from installing printer drivers" security option to "Enabled"	Enabled

Section 24: Security Options (Domain Controllers)

❌	24.01	Failed	Set the "Domain controller: Allow server operators to schedule tasks" security option to "Disabled" on domain controllers	Not Defined
❌	24.02	Failed	Set the "Domain controller: LDAP server signing requirements" security option to "Require signing" on domain controllers	None
❌	24.03	Failed	Set the "Domain controller: Refuse machine account password changes" security option to "Disabled" on domain controllers	Not Defined

Section 25: Security Options (Domain Members)

✅	25.01	Passed	Set the "Domain member: Digitally encrypt or sign secure channel data (always)" security option to "Enabled" on domain members	Enabled
✅	25.02	Passed	Set the "Domain member: Digitally encrypt secure channel data (when possible)" security option to "Enabled" on domain members	Enabled

✓ 25.03	Passed	Set the "Domain member: Digitally sign secure channel data (when possible)" security option to "Enabled" on domain members	Enabled
✓ 25.04	Passed	Set the "Domain member: Disable machine account password changes" security option to "Disabled" on domain members	Disabled
✓ 25.05	Passed	Set the "Domain member: Maximum machine account password age" security option to 30 days on domain members	30 days
✓ 25.06	Passed	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	Failed	Set the "AutoPlay Policies: Disallow Autoplay for non-volume devices" security option to "Enabled"	Not Defined
✗ 26.02	Failed	Set the "AutoPlay Policies: Set the default behavior for AutoRun" security option to "Do not execute any autorun commands"	Not Defined
✗ 26.03	Failed	Set the "AutoPlay Policies: Turn off Autoplay" security option to "All drives"	Not Defined
✗ 26.04	Failed	Set the "File Explorer: Configure Microsoft Defender SmartScreen" security option to "Warn and prevent bypass"	Not Defined
✗ 26.05	Failed	Set the "File Explorer: Enable Microsoft Defender SmartScreen" security option to "Enabled"	Not Defined
✗ 26.06	Failed	Set the "File Explorer: Turn off Data Execution Prevention for Explorer" security option to "Disabled"	Not Defined
✓ 26.07	Passed	Set the "File Explorer: Turn off heap termination on corruption" security option to "Disabled" or "Not Defined"	Not Defined
✓ 26.08	Passed	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	Failed	Set the "Group Policy: Continue experiences on this device" security option to "Disabled" on domain members	Not Defined
✗ 27.02	Failed	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	Failed	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	Passed	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	Failed	Set the "Interactive logon: Don't display last signed-in" security option to "Enabled"	Disabled
✅ 28.02	Passed	Set the "Interactive logon: Do not require CTRL+ALT+DEL" security option to "Disabled"	Disabled
❌ 28.03	Failed	Set the "Interactive logon: Machine account lockout threshold" security option to a value between 6 and 10.	Not Defined
❌ 28.04	Failed	Set the "Interactive logon: Machine inactivity limit" security option to 900 seconds or less	Not Defined
👤 28.05	Manual	Set the "Interactive logon: Message text for users attempting to log on" security option to an appropriate value	
👤 28.06	Manual	Set the "Interactive logon: Message title for users attempting to log on" security option to an appropriate value	
✅ 28.08	Passed	Set the "Interactive logon: Prompt user to change password before expiration" security option to a value between 5 and 10 days	5 days
❌ 28.10	Failed	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	Failed	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	Failed	Set the "Internet Explorer: Prevent downloading of enclosures" security option to "Enabled"	Not Defined

Section 30: Security Options (Lanman Workstation)

❌ 30.01	Failed	Set the "Lanman Workstation: Enable insecure guest logons" security option to "Disabled"	Not Defined
---------	--------	--	-------------

Section 31: Security Options (Logon)

❌ 31.01	Failed	Set the "Logon: Block user from showing account details on sign-in" security option to "Enabled"	Not Defined
❌ 31.02	Failed	Set the "Logon: Do not display network selection UI" security option to "Enabled"	Not Defined
❌ 31.03	Failed	Set the "Logon: Do not enumerate connected users on domain-joined computers" security option to "Enabled" on domain members	Not Defined
❌ 31.05	Failed	Set the "Logon: Turn off app notifications on the lock screen" security option to "Enabled"	Not Defined
❌ 31.06	Failed	Set the "Logon: Turn off picture password sign-in" security option to "Enabled" on domain members	Not Defined
❌ 31.07	Failed	Set the "Logon: Turn on convenience PIN sign-in" security option to "Disabled" on domain members	Not Defined

✓ 31.08	Passed	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	Failed	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	Failed	Set the "Microsoft Defender Antivirus: Configure detection for potentially unwanted applications" security option to "Block"	Not Defined
✓ 33.02	Passed	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	Failed	Set the "Microsoft Defender Antivirus: Configure Watson events" security option to "Disabled"	Not Defined
✓ 33.04	Passed	Set the "Microsoft Defender Antivirus: Join Microsoft MAPS" security option to "Disabled" or "Not Defined"	Not Defined
✗ 33.05	Failed	Set the "Microsoft Defender Antivirus: Prevent users and apps from accessing dangerous websites" security option to "Block"	Not Defined
✗ 33.06	Failed	Set the "Microsoft Defender Antivirus: Scan removable drives" security option to "Enabled"	Not Defined
✓ 33.07	Passed	Set the "Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus" security option to "Disabled" or "Not Defined"	Not Defined
✓ 33.08	Passed	Set the "Microsoft Defender Antivirus: Turn on behavior monitoring" security option to "Enabled" or "Not Defined"	Not Defined
✗ 33.09	Failed	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	Failed	Set the "Microsoft network client: Digitally sign communications (always)" security option to "Enabled"	Not Defined
✓ 34.02	Passed	Set the "Microsoft network client: Digitally sign communications (if server agrees)" security option to "Enabled"	Enabled
✓ 34.03	Passed	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	Passed	Set the "Microsoft network server: Amount of idle time required before suspending session" security option to "15 minutes"	15 minutes
✓ 35.02	Passed	Set the "Microsoft network server: Digitally sign communications (always)" security option to "Enabled"	Enabled

✓	35.03	Passed	Set the "Microsoft network server: Digitally sign communications (if client agrees)" security option to "Enabled"	Enabled
✓	35.04	Passed	Set the "Microsoft network server: Disconnect clients when logon hours expire" security option to "Enabled"	Enabled
✗	35.05	Failed	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	Passed	Set the "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)" security option to "Disabled" or "Not Defined"	Not Defined
✗	36.02	Failed	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	Failed	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	Failed	Set the "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" security option to "Disabled"	Enabled
✗	36.05	Failed	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	Failed	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	Failed	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	Passed	Set the "MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)" security option to "Enabled" or "Not Defined"	Not Defined
✗	36.09	Failed	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	Failed	Set the "MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted" security option to 3	Not Defined
✗	36.11	Failed	Set the "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted" security option to 3	Not Defined
✗	36.12	Failed	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	Failed	Set the "DNS Client: Turn off multicast name resolution" security option to "Enabled"	Not Defined
❌ 37.02	Failed	Set the "TCP/IP: NetBT NodeType" security option to "P-node (recommended)"	Not Defined

Section 38: Security Options (Network Access)

✅ 38.01	Passed	Set the "Network access: Allow anonymous SID/Name translation" security option to "Disabled" (must be set with Group Policy)	Disabled
❌ 38.02	Failed	Set the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" security option to "Enabled"	Disabled
✅ 38.03	Passed	Set the "Network access: Do not allow anonymous enumeration of SAM accounts" security option to "Enabled"	Enabled
❌ 38.04	Failed	Set the "Network access: Do not allow storage of passwords and credentials for network authentication" security option to "Enabled"	Disabled
✅ 38.05	Passed	Set the "Network access: Let Everyone permissions apply to anonymous users" security option to "Disabled"	Disabled
❌ 38.06	Failed	Set the "Network access: Named Pipes that can be accessed anonymously" security option to only contain [Empty]	netlogon samr lsarpc
✅ 38.07	Passed	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	Passed	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

		System\CurrentControlSet\Control\Server Applications	
✓ 38.09	Passed	Set the "Network access: Restrict anonymous access to Named Pipes and Shares" security option to "Enabled"	Enabled
✗ 38.11	Failed	Set the "Network access: Shares that can be accessed anonymously" security option to an empty value	Not Defined
✓ 38.12	Passed	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	Failed	Set the "Network Connections: Prohibit installation and configuration of Network Bridge on your DNS domain network" security option to "Enabled"	Not Defined
✗ 39.02	Failed	Set the "Network Connections: Prohibit use of Internet Connection Sharing on your DNS domain network" security option to "Enabled"	Not Defined
✗ 39.03	Failed	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	Passed	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	Failed	Set the "Network security: Allow Local System to use computer identity for NTLM" security option to "Enabled"	Not Defined
✗ 41.02	Failed	Set the "Network security: Allow LocalSystem NULL session fallback" security option to "Disabled"	Not Defined
✗ 41.03	Failed	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	Failed	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	Passed	Set the "Network security: Do not store LAN Manager hash value on next password change" security option to "Enabled"	Enabled
✗ 41.06	Failed	Set the "Network security: Force logoff when logon hours expire" security option to "Enabled"	Disabled
✗ 41.07	Failed	Set the "Network security: LAN Manager authentication level" security option to "Send NTLMv2 response only. Refuse LM & NTLM"	Not Defined

❌ 41.08	Failed	Set the "Network security: LDAP client signing requirements" security option to "Require Signing"	Negotiate Signing
❌ 41.09	Failed	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	Failed	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	Failed	Set the "Personalization: Prevent enabling lock screen camera" security option to "Enabled"	Not Defined
❌ 42.02	Failed	Set the "Personalization: Prevent enabling lock screen slide show" security option to "Enabled"	Not Defined

Section 43: Security Options (Recovery Console)

✅ 43.01	Passed	Set the "Recovery console: Allow automatic administrative logon" security option to "Disabled"	Disabled
✅ 43.02	Passed	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	Failed	Set the "Remote Assistance: Allow Offer Remote Assistance" security option to "Disabled"	Not Defined
❌ 44.02	Failed	Set the "Remote Assistance: Allow Solicited Remote Assistance" security option to "Disabled"	Not Defined

Section 45: Security Options (Remote Desktop Connection Client)

❌ 45.01	Failed	Set the "Remote Desktop Connection Client: Do not allow passwords to be saved" security option to "Enabled"	Not Defined
---------	--------	---	-------------

Section 47: Security Options (Search)

❌ 47.01	Failed	Set the "Search: Allow Cloud Search" security option to "Disable Cloud Search"	Not Defined
✅ 47.02	Passed	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	Passed	Set the "Security Providers: WDigest Authentication" security option to "Disabled" or "Not Defined"	Not Defined
---------	--------	---	-------------

Section 49: Security Options (Startup and Shutdown)

✓ 49.01	Passed	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	Passed	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	Failed	Set the "Shutdown: Clear virtual memory pagefile" security option to "Enabled"	Disabled

Section 50: Security Options (System Cryptography)

✗ 50.01	Failed	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	Passed	Set the "System objects: Require case insensitivity for non-Windows subsystems" security option to "Enabled"	Enabled
✓ 51.02	Passed	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	Passed	Set the "System settings: Optional subsystems" security option to include only [Empty]	
✗ 52.02	Failed	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	Failed	Set the "User Account Control: Admin Approval Mode for the Built-in Administrator account" security option to "Enabled"	Not Defined
✓ 53.02	Passed	Set the "User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop" security option to "Disabled"	Disabled
✗ 53.03	Failed	Set the "User Account Control: Apply UAC restrictions to local accounts on network logons" security option to "Enabled"	Not Defined
✗ 53.04	Failed	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	Failed	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	Passed	Set the "User Account Control: Detect application installations and prompt for elevation" security option to "Enabled"	Enabled

✓ 53.07	Passed	Set the "User Account Control: Only elevate UIAccess applications that are installed in secure locations" security option to "Enabled"	Enabled
✓ 53.08	Passed	Set the "User Account Control: Run all administrators in Admin Approval Mode" security option to "Enabled"	Enabled
✓ 53.09	Passed	Set the "User Account Control: Switch to the secure desktop when prompting for elevation" security option to "Enabled"	Enabled
✓ 53.10	Passed	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	Passed	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	Failed	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	Passed	Set the "Windows Installer: Allow user control over installs" security option to "Disabled" or "Not Defined"	Not Defined
✓ 55.02	Passed	Set the "Windows Installer: Always install with elevated privileges" security option to "Disabled" or "Not Defined"	Not Defined
✓ 55.03	Passed	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	Failed	Set the "Windows PowerShell: Turn on PowerShell Script Block Logging" security option to "Enabled"	Not Defined
✗ 56.02	Failed	Set the "Windows PowerShell: Turn on PowerShell Transcription" security option to "Enabled"	Not Defined

Section 57: Security Options (Windows Security)

✗ 57.01	Failed	Set the "Windows Security: App and browser protection: Prevent users from modifying settings" security option to "Enabled"	Not Defined
---------	--------	--	-------------



Hardware

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

Hardware Information

Serial Number	VMware-56 4d 4f 0e f3 9a ef 95-ed 03 ca f3 02 f9 14 fe
Manufacturer	VMware, Inc.
Model	VMware20,1
Asset Tag	

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	2 Processors
Total Physical Memory	4,095MB
UUID	0E4F4D56-9AF3-95EF-ED03-CAF302F914FE

BIOS

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

 VMW201.00V.25600138.B64.2607151225

Manufacturer	VMware, Inc.
Release Date	15 July 2026 01:00:00
SMBIOS BIOS Version	VMW201.00V.25600138.B64.2607151225
Version	INTEL - 6040000
Current Language	
Embedded Controller Version	255.255.0.0
Firmware Type	UEFI
System BIOS Version	255.255.0.0



Devices

Provides details about the devices and drivers on this machine.

2 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.

1 Batteries

Name	Driver Provider	Driver Version	Status
 Microsoft AC Adapter	Microsoft	10.0.26100.33438	Device is working properly.

2 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.

2 Disk drives

Name	Driver Provider	Driver Version	Status
 VMware Virtual NVMe Disk	Microsoft	10.0.26100.7309	Device is working properly.
 VMware, VMware Virtual S SCSI Disk Device	Microsoft	10.0.26100.7309	Device is working properly.

1 Display adapters

Name	Driver Provider	Driver Version	Status
 VMware SVGA 3D	Broadcom Inc.	9.17.11.4	Device is working properly.

1 DVD/CD-ROM drives

Name	Driver Provider	Driver Version	Status
 NECVMWar VMware SATA CD01	Microsoft	10.0.26100.33438	Device is working properly.

2 Firmware

Name	Driver Provider	Driver Version	Status
 EFI Firmware From Host	Broadcom Inc.	1.0.0.3	Device is working properly.
 Platform Key Firmware From Host	Broadcom Inc.	1.0.0.0	Device is working properly.

2 Human Interface Devices

Name	Driver Provider	Driver Version	Status
 USB Input Device	Microsoft	10.0.26100.33438	Device is working properly.
 USB Input Device	Microsoft	10.0.26100.33438	Device is working properly.

4 IDE ATA/ATAPI controllers

Name	Driver Provider	Driver Version	Status
 ATA Channel 0	Microsoft	10.0.26100.7309	Device is working properly.
 ATA Channel 1	Microsoft	10.0.26100.7309	Device is working properly.
 Intel(R) 82371AB/EB PCI Bus Master IDE Controller	Microsoft	10.0.26100.7309	Device is working properly.
 Standard SATA AHCI Controller	Microsoft	10.0.26100.7309	Device is working properly.

1 Keyboards

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

3 Mice and other pointing devices

Name	Driver Provider	Driver Version	Status
 VMware Pointing Device	Broadcom Inc.	12.5.15.0	Device is working properly.
 VMware USB Pointing Device	Broadcom Inc.	12.5.15.0	Device is working properly.
 VMware USB Pointing Device	Broadcom Inc.	12.5.15.0	Device is working properly.

1 Monitors

Name	Driver Provider	Driver Version	Status
 Generic Monitor	Microsoft	10.0.26100.33438	Device is working properly.

2 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	10.0.26100.32860	Device is working properly.

1 Portable Devices

Name	Driver Provider	Driver Version	Status
 Data	Microsoft	10.0.26100.5074	Device is working properly.

2 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.

2 Processors

Name	Driver Provider	Driver Version	Status
 11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz	Microsoft	10.0.26100.33438	Device is working properly.
 11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz	Microsoft	10.0.26100.33438	Device is working properly.

1 Software components

Name	Driver Provider	Driver Version	Status
 Generic software component	Microsoft	10.0.26100.1	Device is working properly.

2 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.

1 Sound, video and game controllers

Name	Driver Provider	Driver Version	Status
 High Definition Audio Device	Microsoft	10.0.26100.32860	Device is working properly.

5 Storage controllers

Name	Driver Provider	Driver Version	Status
 LSI Adapter, SAS 3000 series, 8-port with 1068	LSI	1.34.3.83	Device is working properly.
 Microsoft iSCSI Target LocalMount Adapter	Microsoft	10.0.26100.1150	Device is working properly.
 Microsoft Storage Spaces Controller	Microsoft	10.0.26100.33438	Device is working properly.
 Microsoft VHD Loopback Controller	Microsoft	10.0.26100.33438	Device is working properly.
 Standard NVMe Express Controller	Microsoft	10.0.26100.33438	Device is working properly.

6 Storage volumes

Name	Driver Provider	Driver Version	Status
 Volume	Microsoft	10.0.26100.5074	Device is working properly.
 Volume	Microsoft	10.0.26100.5074	Device is working properly.
 Volume	Microsoft	10.0.26100.5074	Device is working properly.
 Volume	Microsoft	10.0.26100.5074	Device is working properly.
 Volume	Microsoft	10.0.26100.5074	Device is working properly.
 Volume	Microsoft	10.0.26100.5074	Device is working properly.

7 Universal Serial Bus controllers

Name	Driver Provider	Driver Version	Status
 Standard Enhanced PCI to USB Host Controller	Microsoft	10.0.26100.33438	Device is working properly.
 Standard Universal PCI to USB Host Controller	Microsoft	10.0.26100.33438	Device is working properly.
 Standard USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)	Microsoft	10.0.26100.33438	Device is working properly.
 USB Composite Device	Microsoft	10.0.26100.33438	Device is working properly.
 USB Root Hub	Microsoft	10.0.26100.33438	Device is working properly.
 USB Root Hub	Microsoft	10.0.26100.33438	Device is working properly.
 USB Root Hub (USB 3.0)	Microsoft	10.0.26100.33438	Device is working properly.

Disk Drives

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

2 Disk Drives

Display Name	Interface	Serial Number	Partition Style	Size
 [0] VMware, VMware Virtual S SCSI Disk Device	Serial Attached SCSI (SAS)		GUID Partition Table (GPT)	60 GB
 [1] VMware Virtual NVMe Disk	NVMe	4DC5_F6A6_17B2_AFAB_000C_2960_5B80_9E40.	GUID Partition Table (GPT)	60 GB

[0] VMware, VMware Virtual S SCSI Disk Device

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

General

Manufacturer	VMware,
Model	VMware, VMware Virtual S SCSI Disk Device
Firmware Revision	1.0
Bus Type	Serial Attached SCSI (SAS)
Serial Number	
Size	60 GB
Location	PCI Slot 256 : Bus 27 : Device 0 : Function 0 : Adapter 0 : Port 0 : Target 0 : LUN 0
GUID	{d3e77308-add9-4fd6-8c38-89657d825538}
Capabilities	Random Access Supports Writing
Partition Style	GUID Partition Table (GPT)
Bytes Per Sector	512
Sectors Per Track	63

Status

Operational Status	OK
--------------------	----

Storage Pools

Storage Pool Names	Primordial
--------------------	------------

Unallocated Space

Unallocated Space	14 MB
-------------------	-------

1 Partitions

Identifier	Active	Type	Size
 Disk #0, Partition #0	False	Basic (GPT)	59.98 GB

 D:

Active	False
Partition ID	Disk #0, Partition #0
Partition Type	Basic (GPT)
File System	NTFS
Volume Name	Data
Volume Serial Number	D6A4132E
Size	59.98 GB

D: (35% free)



[1] VMware Virtual NVMe Disk

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

 General

Model	VMware Virtual NVMe Disk
Firmware Revision	1.4
Bus Type	NVMe
Serial Number	4DC5_F6A6_17B2_AFAB_000C_2960_5B80_9E40.
Size	60 GB
Location	nvme0
GUID	{dd7eb22e-3dde-4a6b-af6b-0b00be169ba8}
Capabilities	Random Access Supports Writing
Partition Style	GUID Partition Table (GPT)
Bytes Per Sector	512
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 #1, Partition #0	True	Other	100 MB
 Disk #1, Partition #1	False	Basic (GPT)	59.04 GB
 Disk #1, Partition #2	False	Other (GPT)	866 MB

 C:

Active	False
Partition ID	Disk #1, Partition #1
Partition Type	Basic (GPT)
File System	NTFS
Volume Name	System
Volume Serial Number	02D7B448
Size	59.04 GB

C: (24% free)



Disk Volumes

Provides information about the disk volumes found on this Windows machine.

 4 Volumes

Name	Total Size	Free Space	Shadow Copy
 C: (System)	59.04 GB	14.2 GB	False
 D: (Data)	59.98 GB	20.76 GB	False
 EFI System Partition (b0bbb371-44e3-439e-a4eb-046083980853)	96 MB	45.59 MB	False
 Recovery Partition (233d1a52-6c14-4f2b-a918-5cfb8ff8ec94)	866 MB	122.36 MB	False

C: (System)

Provides information about the disk volumes found on this Windows machine.

 Volume Details

Block Size	4,096
Capacity	59.04 GB
Drive Letter	C:
File System	NTFS
Label	System
Volume Identifier	b5182077-2111-4303-bc86-565bc66be877
Used Space	44.84 GB
Free Space	14.2 GB

C: (System) (24% free)



 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 Directories	This folder and subfolders
 BUILTIN\Users	False	Allow	Create Files	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	Execute File List Directory Read attributes	This folder or file only

0 NTFS Audit Rules

There are no audit rules found.

D: (Data)

Provides information about the disk volumes found on this Windows machine.

 Volume Details

Block Size	4,096
Capacity	59.98 GB
Drive Letter	D:
File System	NTFS
Label	Data
Volume Identifier	b0a44f62-ac87-40a7-91b3-4c87c11236c2
Used Space	39.22 GB
Free Space	20.76 GB

D: (Data) (35% free)



 Shadow Copy Configuration

Enabled	False
---------	-------

 Disk Quota

State	Disabled
-------	----------

 Security

Owner	NT AUTHORITY\SYSTEM
-------	---------------------

 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	Create Directories	This folder and subfolders
 BUILTIN\Users	False	Allow	Create Files	Subfolders only
 BUILTIN\Users	False	Allow	Read & execute	This folder, subfolders and files
 CREATOR OWNER	False	Allow	Full control	Subfolders and files only
 Everyone	False	Allow	Read & execute	This folder or file only
 NT AUTHORITY\SYSTEM	False	Allow	Full control	This folder, subfolders and files



0 NTFS Audit Rules

There are no audit rules found.

EFI System Partition (b0bbb371-44e3-439e-a4eb-046083980853)

Provides information about the disk volumes found on this Windows machine.

 Volume Details

Block Size	1,024
Capacity	96 MB
Drive Letter	
File System	FAT32
Label	
Volume Identifier	b0bbb371-44e3-439e-a4eb-046083980853
Used Space	50.41 MB
Free Space	45.59 MB

EFI System Partition (b0bbb371-44e... (47% free)



 Shadow Copy Configuration

Enabled	False
---------	-------

Recovery Partition (233d1a52-6c14-4f2b-a918-5cfb8ff8ec94)

Provides information about the disk volumes found on this Windows machine.

 Volume Details

Block Size	4,096
Capacity	866 MB
Drive Letter	
File System	NTFS
Label	
Volume Identifier	233d1a52-6c14-4f2b-a918-5cfb8ff8ec94
Used Space	743.64 MB
Free Space	122.36 MB

Recovery Partition (233d1a52-6c14-... (14% free)



 Shadow Copy Configuration

Enabled	False
---------	-------

Optical 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
 O:	NECVMWar VMware SATA CD01	DVD-ROM	(Standard CD-ROM drives)	Random Access Supports Removable Media

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]
------------	--------------

6 Permissions

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

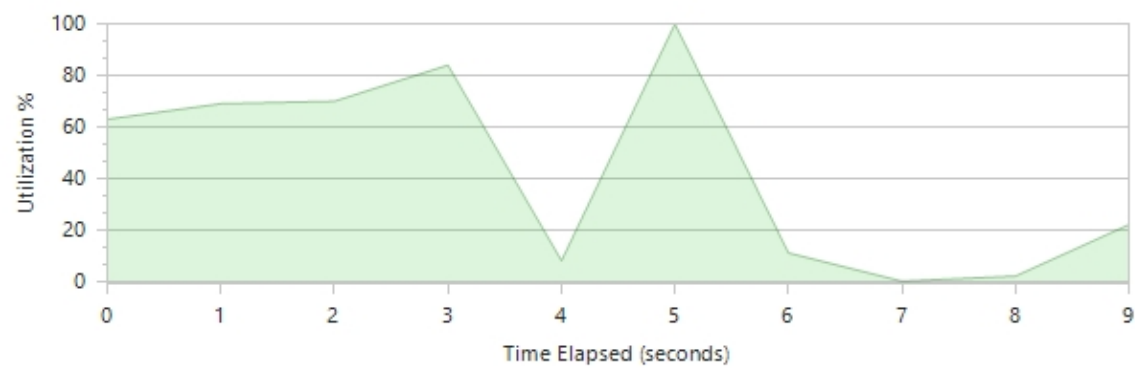
Processors

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

2 Processors

Device ID	Name	Status	Cores
 CPU0	11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz	Enabled	1
 CPU1	11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz	Enabled	1

Total Processor Utilization



11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz

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

11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz

CPU Status	Enabled
Current Clock Speed	2,496MHz
Description	Intel64 Family 6 Model 141 Stepping 1
Device Identifier	CPU0
Manufacturer	GenuineIntel
Number Of Cores	1
Number Of Logical Processors	1
Processor Id	0F8BFBF000806D1
Socket Designation	CPU 0

Cache Information

Level 2 Cache Size	1,280KB
Level 3 Cache Size	24,576KB

Virtualization Settings

Address Translation Extensions	False
Virtualization Firmware Enabled	False

11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz

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

11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz

CPU Status	Enabled
Current Clock Speed	2,496MHz
Description	Intel64 Family 6 Model 141 Stepping 1
Device Identifier	CPU1
Manufacturer	GenuineIntel
Number Of Cores	1
Number Of Logical Processors	1
Processor Id	0F8BFBF000806D1
Socket Designation	CPU 1

Cache Information

Level 2 Cache Size	1,280KB
Level 3 Cache Size	24,576KB

Virtualization Settings

Address Translation Extensions	False
Virtualization Firmware Enabled	False

Trusted Platform Module (TPM)

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

 Trusted Platform Module (TPM)

TPM Present	False
-------------	-------

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 Adapters

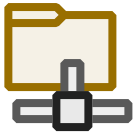
Name	Adapter Memory	Driver Version
 VMware SVGA 3D	256 MB	9.17.11.4

VMware SVGA 3D

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.

 VMware SVGA 3D

DAC Type	n/a
Adapter RAM	256 MB
Driver Date	01 June 2026 01:00:00
Driver Version	9.17.11.4
Inf Filename	oem2.inf
Drivers	C:\WINDOWS\System32\DriverStore\FileRepository\vm3d.inf_amd64_39d3dfd189710365\vm3dum64_loader.dll
Maximum Refresh Rate	64Hz
Video Mode Description	1477 x 1040 x 4294967296 colors



Networking

Provides networking information for the Windows machine.



Networking Information

Network Adapters	5 Network Adapters
IPv4 Addresses	192.168.176.132/24
IPv6 Addresses	fe80::7900:9a83:7941:7a91%5/0.0.0.64



Advanced

SNMP Installed	False
Routing Table Entries	11
Shares	7

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	False
---------	-------

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	01 April 2024 08:01:27
Last Accessed	01 April 2024 08:01:27
Last Modified	01 April 2024 08:01:27
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.



```
# 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
 192.168.176.255	255.255.255.255	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
 192.168.176.132	255.255.255.255	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
 192.168.176.0	255.255.255.0	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	192.168.176.2	Intel(R) 82574L Gigabit Network Connection	281	NetMgmt

1 Persistent Routes

Destination	Subnet Mask	Gateway	Metric
 0.0.0.0	0.0.0.0	192.168.176.2	256

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.

 1 Network Adapters

Name	Status	Device Name	MAC address
 Ethernet0	Device is working properly.	Intel(R) 82574L Gigabit Network Connection	00-0C-29-F9-14-FE

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	0005
Device Name	Intel(R) 82574L Gigabit Network Connection
MAC Address	00-0C-29-F9-14-FE
Status	Device is working properly.
Driver Date	2015-08-03
Driver Version	12.19.1.32
Physical Adapter	True
Interface GUID	{B6DB7048-1353-4352-9E56-DB2116C1395A}
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 LLD 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	False
IP Addresses	fe80::7900:9a83:7941:7a91%5/0.0.0.64 192.168.176.132/24
Default Gateways	192.168.176.2

DNS Settings

DNS Hostname	CSDEMO-DC01
DNS Domain	
DNS Suffixes	centresolutionsdemo.int
DNS Servers	127.0.0.1 ::1
Register in DNS	True
Use Connection's Suffix in DNS Registration	False

WINS Settings

Primary WINS Server	
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

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

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).

 7 Shares

Name	Path	Type	Description
 ADMIN\$	C:\WINDOWS	Administrative Share	Remote Admin
 C\$	C:\	Administrative Share	Default share
 D\$	D:\	Administrative Share	Default share
 IPC\$		Administrative IPC Queue	Remote IPC
 NETLOGON	C:\WINDOWS\SYSVOL\sysvol\centrelsolutionsdemo.int\SCRIPTS	File Share	Logon server share
 Public	D:\DFSRoots\Public	File Share	
 SYSVOL	C:\WINDOWS\SYSVOL\sysvol	File Share	Logon server share

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\$

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 Directories	This folder and subfolders
 BUILTIN\Users	False	Allow	Create Files	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	Execute File List Directory Read attributes	This folder or file only

0 NTFS Audit Rules

There are no audit rules found.

 D\$

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

 Security

Owner	NT AUTHORITY\SYSTEM
-------	---------------------

 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	Create Directories	This folder and subfolders
 BUILTIN\Users	False	Allow	Create Files	Subfolders only
 BUILTIN\Users	False	Allow	Read & execute	This folder, subfolders and files
 CREATOR OWNER	False	Allow	Full control	Subfolders and files only
 Everyone	False	Allow	Read & execute	This folder or file only
 NT AUTHORITY\SYSTEM	False	Allow	Full control	This folder, subfolders and files

 0 NTFS Audit Rules

There are no audit rules found.

IPC\$

 IPC\$

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

NETLOGON

NETLOGON

Description	Logon server share
Allow Maximum	True
Path	C:\WINDOWS\SYSVOL\sysvol\centrelsolutionsdemo.int\SCRIPTS
Share Type	File Share
Cache Setting	Only files and folders that users specify are available offline.
Enable Access Based Enumeration	False
Encrypt Data Access	False

2 Share Permissions

Account Name	Action	Rights
 Everyone	Allow	Read
 BUILTIN\Administrators	Allow	Full Control

Security

Owner	BUILTIN\Administrators
-------	------------------------

6 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
 BUILTIN\Administrators	False	Allow	Full control	Subfolders and files only
 BUILTIN\Administrators	False	Allow	Change permissions Read & execute Take ownership Write	This folder or file only
 BUILTIN\Server Operators	False	Allow	Read & execute	This folder, subfolders and files
 CREATOR OWNER	False	Allow	Full control	Subfolders and files only
 NT AUTHORITY\Authenticated Users	False	Allow	Read & execute	This folder, subfolders and files
 NT AUTHORITY\SYSTEM	False	Allow	Full control	This folder, subfolders and files

1 NTFS Audit Rules

Account Name	Inherited	Type	Rights	Applies To
 Everyone	False	Success	Delete	This folder or file only

Public

 Public

Description	
Allow Maximum	True
Path	D:\DFSRoots\Public
Share Type	File Share
Cache Setting	Only files and folders that users specify are available offline.
Enable Access Based Enumeration	False
Encrypt Data Access	False

 1 Share Permissions

Account Name	Action	Rights
 Everyone	Allow	Read

 Security

Owner	BUILTIN\Administrators
-------	------------------------

 6 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
 BUILTIN\Administrators	False	Allow	Full control	This folder or file only
 BUILTIN\Administrators	True	Allow	Full control	This folder, subfolders and files
 BUILTIN\Users	True	Allow	Read & execute	This folder, subfolders and files
 BUILTIN\Users	True	Allow	Create Directories Create Files	This folder and subfolders
 CREATOR OWNER	True	Allow	Full control	Subfolders and files only
 NT AUTHORITY\SYSTEM	True	Allow	Full control	This folder, subfolders and files

 0 NTFS Audit Rules

There are no audit rules found.

SYSVOL



Description	Logon server share
Allow Maximum	True
Path	C:\WINDOWS\SYSVOL\sysvol
Share Type	File Share
Cache Setting	Only files and folders that users specify are available offline.
Enable Access Based Enumeration	False
Encrypt Data Access	False

3 Share Permissions

Account Name	Action	Rights
Everyone	Allow	Read
BUILTIN\Administrators	Allow	Full Control
NT AUTHORITY\Authenticated Users	Allow	Full Control

Security

Owner	BUILTIN\Administrators
-------	------------------------

5 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
BUILTIN\Administrators	False	Allow	Change permissions Read & execute Take ownership Write	This folder, subfolders and files
BUILTIN\Server Operators	False	Allow	Read & execute	This folder, subfolders and files
CREATOR OWNER	False	Allow	Change permissions Read & execute Take ownership Write	Subfolders and files only
NT AUTHORITY\Authenticated Users	False	Allow	Read & execute	This folder, subfolders and files
NT AUTHORITY\SYSTEM	False	Allow	Full control	This folder, subfolders and files



1 NTFS Audit Rules

Account Name	Inherited	Type	Rights	Applies To
 Everyone	False	Success	Delete	This folder, subfolders and files

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
-----------	-------



Security

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

 Security Identifiers

Machine SID	S-1-5-21-3339536540-746212746-1526301273
Computer Domain SID	S-1-5-21-3339536540-746212746-1526301273-1000

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.

 Audit Policy

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

Certificates

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

 6 Certificate Stores

Store Name	Certificate Count
 Intermediate Certification Authorities	5
 Personal	2
 Third-Party Root Certification Authorities	8
 Trusted People	0
 Trusted Publisher	2
 Trusted Root Certification Authorities	13

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.

 2 Certificates

Issued To	Issuer	Expiry Date
 157f8a9e-052c-4fc2-8b9f-11e8ccc55e96	HISConnectorRegistrationCA.his.msapproxy.net	26 September 2026
 WindowsAdminCenterSelfSigned	WindowsAdminCenterSelfSigned	17 October 2026

157f8a9e-052c-4fc2-8b9f-11e8ccc55e96

Provides details of the X.509 certificate.

General

Archived	False
Subject Name	157f8a9e-052c-4fc2-8b9f-11e8ccc55e96
Subject	CN=157f8a9e-052c-4fc2-8b9f-11e8ccc55e96
Has Private Key	True
Issuer	CN=HISConnectorRegistrationCA.his.msapproxy.net
Issuer Name	HISConnectorRegistrationCA.his.msapproxy.net
Valid From	13 April 2026
Expiry Date	26 September 2026
Key Usage	
Enhanced Key Usages	Client Authentication (1.3.6.1.5.5.7.3.2)

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	F60B883E170B148643DAC5383BC316F6
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	
Thumbprint	F9146B369F1C0B5A70A587A776D1DEC5F9A52F54
Purposes	Enable all purposes for this certificate

WindowsAdminCenterSelfSigned

Provides details of the X.509 certificate.

 General

Archived	False
Subject Name	WindowsAdminCenterSelfSigned
Subject	CN=WindowsAdminCenterSelfSigned
Has Private Key	True
Issuer	CN=WindowsAdminCenterSelfSigned
Issuer Name	WindowsAdminCenterSelfSigned
Valid From	18 August 2026
Expiry Date	17 October 2026
Key Usage	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	2D186DADC0705A894C4F4A42CAC47ED8
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	CSDEMO-DC01.centrelsolutionsdemo.int

 Properties

Friendly Name	Windows Admin Center Self-Signed Certificate
Thumbprint	DFF3DF5A74473D3470A1F2A43C3EF87CD9375330
Purposes	Enable all purposes for this certificate

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

Microsoft Defender

Provides information about the detected antivirus (also known as antimalware) products found on this Windows machine.

General Settings

Product Version	4.18.26080.4
Engine Version	1.1.26080.3
Real Time Protection Enabled	True
Tamper Protection	False

Antivirus Signature

Antivirus Signature Last Updated	17 September 2026 21:54:17
Antivirus Signature Version	1.459.263.0

Cloud

Cloud Delivered Protection Enabled	True
Automatic Cloud Sample Submission	True

Exclusions

Excluded Extensions	
Excluded Paths	
Excluded Processes	

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	None	Default Domain Controllers Policy
 Domain controller: Refuse machine account password changes	Not Defined	Not Defined
 Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Default Domain Controllers Policy
 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	Disabled	Configured Locally
 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	Not Defined	Not Defined
 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)	Enabled	Default Domain Controllers Policy
 Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Default Domain Controllers Policy

 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)	Not Defined	Not Defined
 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	netlogon samr lsarpc	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 Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\SysmonLog	Configured Locally
 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	Default Domain Controllers Policy	BUILTIN\Administrators BUILTIN\Pre-Windows 2000 Compatible Access Everyone NT AUTHORITY\Authenticated Users NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
 Act as part of the operating system	SeTcbPrivilege	Configured Locally	
 Add workstations to domain	SeMachineAccountPrivilege	Default Domain Controllers Policy	NT AUTHORITY\Authenticated Users
 Adjust memory quotas for a process	SeIncreaseQuotaPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE
 Allow log on locally	SeInteractiveLogonRight	Default Domain Controllers Policy	BUILTIN\Account Operators BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Print Operators BUILTIN\Server Operators NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
 Allow log on through Remote Desktop Services	SeRemoteInteractiveLogonRight	Configured Locally	BUILTIN\Administrators
 Back up files and directories	SeBackupPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators
 Bypass traverse checking	SeChangeNotifyPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators

			BUILTIN\Pre-Windows 2000 Compatible Access Everyone NT AUTHORITY\Authenticated Users NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE RESTRICTED SERVICES\PrintSpoolerService
 Change the system time	SeSystemtimePrivilege	Default Domain Controllers Policy	BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE
 Change the time zone	SeTimeZonePrivilege	Configured Locally	BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE
 Create a pagefile	SeCreatePagefilePrivilege	Default Domain Controllers Policy	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	Default Domain Controllers Policy	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	Default Domain Controllers Policy	BUILTIN\Administrators

 Force shutdown from a remote system	SeRemoteShutdownPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators BUILTIN\Server Operators
 Generate security audits	SeAuditPrivilege	Default Domain Controllers Policy	NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE RESTRICTED SERVICES\PrintSpoolerService
 Impersonate a client after authentication	SeImpersonatePrivilege	Configured Locally	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE RESTRICTED SERVICES\PrintSpoolerService
 Increase a process working set	SeIncreaseWorkingSetPrivilege	Configured Locally	BUILTIN\Users
 Increase scheduling priority	SeIncreaseBasePriorityPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators Window Manager\Window Manager Group
 Load and unload device drivers	SeLoadDriverPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators BUILTIN\Print Operators
 Lock pages in memory	SeLockMemoryPrivilege	Configured Locally	
 Log on as a batch job	SeBatchLogonRight	Default Domain Controllers Policy	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Performance Log Users
 Log on as a service	SeServiceLogonRight	Configured Locally	CSDemo\Administrator CSDemo\pGMSA_c2ca7496\$ CSDemo\XiaClient NT SERVICE\ALL SERVICES NT SERVICE\himds RESTRICTED SERVICES\ALL RESTRICTED SERVICES
 Manage auditing and security log	SeSecurityPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators CSDemo\Exchange Servers
 Modify an object label	SeRelabelPrivilege	Configured Locally	
 Modify firmware environment values	SeSystemEnvironmentPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators

 Perform volume maintenance tasks	SeManageVolumePrivilege	Configured Locally	BUILTIN\Administrators
 Profile single process	SeProfileSingleProcessPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators
 Profile system performance	SeSystemProfilePrivilege	Default Domain Controllers Policy	BUILTIN\Administrators NT SERVICE\WdiServiceHost
 Remove computer from docking station	SeUndockPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators
 Replace a process-level token	SeAssignPrimaryTokenPrivilege	Default Domain Controllers Policy	NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE
 Restore files and directories	SeRestorePrivilege	Default Domain Controllers Policy	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators
 Shut down the system	SeShutdownPrivilege	Default Domain Controllers Policy	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Print Operators BUILTIN\Server Operators
 Synchronize directory service data	SeSyncAgentPrivilege	Configured Locally	
 Take ownership of files or other objects	SeTakeOwnershipPrivilege	Default Domain Controllers Policy	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.

163 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
 Active Directory Domain Controller - Echo Request (ICMPv4-In)	Any	ICMPv4	Any	RPC	Any	Any
 Active Directory Domain Controller - Echo Request (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
 Active Directory Domain Controller - LDAP (TCP-In)	Any	TCP	Any	389	Any	Any
 Active Directory Domain Controller - LDAP (UDP-In)	Any	UDP	Any	389	Any	Any
 Active Directory Domain Controller - LDAP for Global Catalog (TCP-In)	Any	TCP	Any	3268	Any	Any
 Active Directory Domain Controller - NetBIOS name resolution (UDP-In)	Any	UDP	Any	138	Any	Any
 Active Directory Domain Controller - SAM/LSA (NP-TCP-In)	Any	TCP	Any	445	Any	Any
 Active Directory Domain Controller - SAM/LSA (NP-UDP-In)	Any	UDP	Any	445	Any	Any
 Active Directory Domain Controller - Secure LDAP (TCP-In)	Any	TCP	Any	636	Any	Any
 Active Directory Domain Controller - Secure LDAP for Global Catalog (TCP-...	Any	TCP	Any	3269	Any	Any
 Active Directory Domain Controller - W32Time (NTP-UDP-In)	Any	UDP	Any	123	Any	Any
 Active Directory Domain Controller (RPC)	Any	TCP	Any	RPC	Any	Any
 Active Directory Domain Controller (RPC-EPMAP)	Any	TCP	Any	RPCMAP	Any	Any
 Active Directory Web Services (TCP-In)	Any	TCP	Any	9389	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)	Public	TCP	Any	10246	PlayToDevice	Any
✓ Cast to Device streaming server (HTTP-Streaming-In)	Domain	TCP	Any	10246	Any	Any
✓ Cast to Device streaming server (HTTP-Streaming-In)	Private	TCP	Any	10246	LocalSubnet	Any
✓ Cast to Device streaming server (RTCP-Streaming-In)	Domain	UDP	Any	Any	Any	Any
✓ Cast to Device streaming server (RTCP-Streaming-In)	Public	UDP	Any	Any	PlayToDevice	Any
✓ Cast to Device streaming server (RTCP-Streaming-In)	Private	UDP	Any	Any	LocalSubnet	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)	Domain	TCP	Any	23554 23555 23556	Any	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
✓ DFS Replication (RPC-EPMAP)	Any	TCP	Any	RPCEPMap	Any	Any
✓ DFS Replication (RPC-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
✓ DNS (TCP, Incoming)	Any	TCP	Any	53	Any	Any
✓ DNS (UDP, Incoming)	Any	UDP	Any	53	Any	Any
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	Domain, Private, Public	ICMPv4	Any	RPC	Any	Any
✓ File and Printer Sharing (Echo Request - ICMPv6-In)	Domain, Private, Public	ICMPv6	Any	RPC	Any	Any
✓ File and Printer Sharing (LLMNR-UDP-In)	Domain, Private, Public	UDP	Any	5355	LocalSubnet	Any
✓ File and Printer Sharing (NB-Datagram-In)	Domain, Private, Public	UDP	Any	138	Any	Any
✓ File and Printer Sharing (NB-Name-In)	Domain, Private, Public	UDP	Any	137	Any	Any
✓ File and Printer Sharing (NB-Session-In)	Domain, Private, Public	TCP	Any	139	Any	Any
✓ File and Printer Sharing (Restrictive) (Echo Request - ICMPv4-In)	Domain	ICMPv4	Any	RPC	Any	Any
✓ File and Printer Sharing (Restrictive) (Echo Request - ICMPv4-In)	Public	ICMPv4	Any	RPC	Any	Any
✓ File and Printer Sharing (Restrictive) (Echo Request - ICMPv6-In)	Domain	ICMPv6	Any	RPC	Any	Any
✓ File and Printer Sharing (Restrictive) (Echo Request - ICMPv6-In)	Public	ICMPv6	Any	RPC	Any	Any
✓ File and Printer Sharing (Restrictive) (LLMNR-UDP-In)	Public	UDP	Any	5355	LocalSubnet	Any

✔ File and Printer Sharing (Restrictive) (LLMNR-UDP-In)	Domain	UDP	Any	5355	LocalSubnet	Any
✔ File and Printer Sharing (Restrictive) (SMB-In)	Domain	TCP	Any	445	Any	Any
✔ File and Printer Sharing (Restrictive) (SMB-In)	Public	TCP	Any	445	Any	Any
✔ File and Printer Sharing (Restrictive) (Spooler Service - RPC)	Public	TCP	Any	RPC	Any	Any
✔ File and Printer Sharing (Restrictive) (Spooler Service - RPC)	Domain	TCP	Any	RPC	Any	Any
✔ File and Printer Sharing (Restrictive) (Spooler Service - RPC-EPMAP)	Domain	TCP	Any	RPCMap	Any	Any
✔ File and Printer Sharing (Restrictive) (Spooler Service - RPC-EPMAP)	Public	TCP	Any	RPCMap	Any	Any
✔ File and Printer Sharing (Restrictive) (Spooler Service Worker - RPC)	Domain	TCP	Any	RPC	Any	Any
✔ File and Printer Sharing (Restrictive) (Spooler Service Worker - RPC)	Public	TCP	Any	RPC	Any	Any
✔ File and Printer Sharing (SMB-In)	Domain, Private, Public	TCP	Any	445	Any	Any
✔ File and Printer Sharing (Spooler Service - RPC)	Domain, Private, Public	TCP	Any	RPC	Any	Any
✔ File and Printer Sharing (Spooler Service - RPC-EPMAP)	Domain, Private, Public	TCP	Any	RPCMap	Any	Any
✔ File and Printer Sharing (Spooler Service Worker - RPC)	Domain, Private, Public	TCP	Any	RPC	Any	Any
✔ File Replication (RPC)	Any	TCP	Any	RPC	Any	Any
✔ File Replication (RPC-EPMAP)	Any	TCP	Any	RPCMap	Any	Any
✔ File Server Remote Management (DCOM-In)	Any	TCP	Any	135	Any	Any
✔ File Server Remote Management (SMB-In)	Any	TCP	Any	445	Any	Any
✔ File Server Remote Management (WMI-In)	Any	TCP	Any	RPC	Any	Any
✔ Google Chrome (mDNS-In)	Any	UDP	Any	5353	Any	Any
✔ iSCSI Target (TCP-In)	Any	TCP	Any	3260	Any	Any

✓ iSCSI Target Service (RPC-In)	Any	TCP	Any	RPCEPMap	Any	Any
✓ Kerberos Key Distribution Center - PCR (TCP-In)	Any	TCP	Any	464	Any	Any
✓ Kerberos Key Distribution Center - PCR (UDP-In)	Any	UDP	Any	464	Any	Any
✓ Kerberos Key Distribution Center (TCP-In)	Any	TCP	Any	88	Any	Any
✓ Kerberos Key Distribution Center (UDP-In)	Any	UDP	Any	88	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 Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any

✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Key Distribution Service (RPC EPMAP)	Any	TCP	Any	RPCEPMap	Any	Any
✓ Microsoft Key Distribution Service (RPC)	Any	TCP	Any	RPC	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
✓ ms-resource:ProductPkgDisplayName	Private	TCP	Any	7000	Any	Any
✓ ms-resource:ProductPkgDisplayName	Public	UDP	Any	7000	Any	Any
✓ ms-resource:ProductPkgDisplayName	Private	UDP	Any	7000	Any	Any
✓ ms-resource:ProductPkgDisplayName	Public	UDP	Any	7000	Any	Any
✓ ms-resource:ProductPkgDisplayName	Private	UDP	Any	7000	Any	Any
✓ ms-resource:ProductPkgDisplayName	Public	TCP	Any	7000	Any	Any

✓ ms-resource:ProductPkgDisplayName	Private	TCP	Any	7000	Any	Any
✓ ms-resource:ProductPkgDisplayName	Public	TCP	Any	7000	Any	Any
✓ OpenSSH SSH Server (sshd)	Private	TCP	Any	22	Any	Any
✓ RPC (TCP, Incoming)	Any	TCP	Any	RPC	Any	Any
✓ RPC Endpoint Mapper (TCP, Incoming)	Any	TCP	Any	RPCMap	Any	Any
✓ Start	Domain, Private	Any	Any	Any	Any	Any
✓ WacInboundOpenException	Domain, Private, Public	TCP	Any	8080	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 Backup (RPC)	Any	TCP	Any	RPC	Any	Any
✓ Windows Backup (RPC-EPMap)	Any	TCP	Any	RPCMap	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
✓ Windows Feature Experience Pack	Domain, Private	Any	Any	Any	Any	Any
✓ Windows Feature Experience Pack	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Windows Management Instrumentation (ASync-In)	Domain, Private, Public	TCP	Any	Any	Any	Any
✓ Windows Management Instrumentation (DCOM-In)	Domain, Private, Public	TCP	Any	135	Any	Any
✓ Windows Management Instrumentation (WMI-In)	Domain, Private, Public	TCP	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
✓ Windows Shell Experience	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
✓ Your account	Domain, Private	Any	Any	Any	Any	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.

104 Windows Firewall Rules

Rule Name	Profile Names	Protocol	Local Addresses	Local Ports	Remote Addresses	Remote Ports
 @{MicrosoftWindows.LKG.AccountsService_1000.26100.2033.0_x64__cw5n1h2txye...	Domain, Private, Public	Any	Any	Any	Any	Any
 @{MicrosoftWindows.LKG.IrisService_1000.26100.2033.0_x64__cw5n1h2txyewy?m...	Domain, Private, Public	Any	Any	Any	Any	Any
 @{MicrosoftWindows.LKG.Search_1000.26100.1742.0_x64__cw5n1h2txyewy?ms-res...	Domain, Private, Public	Any	Any	Any	Any	Any
 @{MicrosoftWindows.LKG.TwinSxS_1000.26100.2033.0_x64__cw5n1h2txyewy?ms-re...	Domain, Private, Public	Any	Any	Any	Any	Any
 Active Directory Domain Controller - Echo Request (ICMPv4-Out)	Any	ICMPv4	Any	RPC	Any	Any
 Active Directory Domain Controller - Echo Request (ICMPv6-Out)	Any	ICMPv6	Any	RPC	Any	Any
 Active Directory Domain Controller (TCP-Out)	Any	TCP	Any	Any	Any	Any
 Active Directory Domain Controller (UDP-Out)	Any	UDP	Any	Any	Any	Any
 Active Directory Web Services (TCP-Out)	Any	TCP	Any	Any	Any	Any
 All Outgoing (TCP)	Any	TCP	Any	Any	Any	Any
 All Outgoing (UDP)	Any	UDP	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
✓ File and Printer Sharing (Echo Request - ICMPv4-Out)	Domain, Private, Public	ICMPv4	Any	RPC	Any	Any
✓ File and Printer Sharing (Echo Request - ICMPv6-Out)	Domain, Private, Public	ICMPv6	Any	RPC	Any	Any
✓ File and Printer Sharing (LLMNR-UDP-Out)	Domain, Private, Public	UDP	Any	Any	LocalSubnet	5355
✓ File and Printer Sharing (NB-Datagram-Out)	Domain, Private, Public	UDP	Any	Any	Any	138
✓ File and Printer Sharing (NB-Name-Out)	Domain, Private, Public	UDP	Any	Any	Any	137
✓ File and Printer Sharing (NB-Session-Out)	Domain, Private, Public	TCP	Any	Any	Any	139

✔ File and Printer Sharing (Restrictive) (Echo Request - ICMPv4-Out)	Public	ICMPv4	Any	RPC	Any	Any
✔ File and Printer Sharing (Restrictive) (Echo Request - ICMPv4-Out)	Domain	ICMPv4	Any	RPC	Any	Any
✔ File and Printer Sharing (Restrictive) (Echo Request - ICMPv6-Out)	Public	ICMPv6	Any	RPC	Any	Any
✔ File and Printer Sharing (Restrictive) (Echo Request - ICMPv6-Out)	Domain	ICMPv6	Any	RPC	Any	Any
✔ File and Printer Sharing (Restrictive) (LLMNR-UDP-Out)	Public	UDP	Any	Any	LocalSubnet	5355
✔ File and Printer Sharing (Restrictive) (LLMNR-UDP-Out)	Domain	UDP	Any	Any	LocalSubnet	5355
✔ File and Printer Sharing (Restrictive) (SMB-Out)	Public	TCP	Any	Any	Any	445
✔ File and Printer Sharing (Restrictive) (SMB-Out)	Domain	TCP	Any	Any	Any	445
✔ File and Printer Sharing (SMB-Out)	Domain, Private, Public	TCP	Any	Any	Any	445
✔ mDNS (UDP-Out)	Private	UDP	Any	Any	LocalSubnet	5353
✔ mDNS (UDP-Out)	Domain	UDP	Any	Any	Any	5353
✔ mDNS (UDP-Out)	Public	UDP	Any	Any	LocalSubnet	5353
✔ Microsoft Content	Domain, Private, Public	Any	Any	Any	Any	Any
✔ Microsoft Media Foundation Network Source OUT [TCP ALL]	Any	TCP	Any	Any	LocalSubnet	554 8554-8558
✔ ms-resource:ProductPkgDisplayName	Private	TCP	Any	7000	Any	Any
✔ ms-resource:ProductPkgDisplayName	Public	TCP	Any	7000	Any	Any
✔ ms-resource:ProductPkgDisplayName	Private	UDP	Any	7000	Any	Any
✔ ms-resource:ProductPkgDisplayName	Public	UDP	Any	7000	Any	Any
✔ ms-resource:ProductPkgDisplayName	Public	TCP	Any	7000	Any	Any
✔ ms-resource:ProductPkgDisplayName	Public	UDP	Any	7000	Any	Any

✓ ms-resource:ProductPkgDisplayName	Private	TCP	Any	7000	Any	Any
✓ ms-resource:ProductPkgDisplayName	Private	UDP	Any	7000	Any	Any
✓ 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, 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 Management Instrumentation (WMI-Out)	Domain, Private, Public	TCP	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 Shell Experience	Domain, Private	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

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
 KB5120232	Security Update	NT AUTHORITY\SYSTEM	17/08/2026
 KB5122870	Security Update	NT AUTHORITY\SYSTEM	15/09/2026
 KB5122871	Security Update	NT AUTHORITY\SYSTEM	18/09/2026
 KB5126052	Update	NT AUTHORITY\SYSTEM	18/09/2026

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	Download updates but let me choose whether to install them
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.

✓ 167 History Items

Action Date	Title	Operation	Result
✓ 16 April 2026 15:11:25	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.136.0) - Current Channel (Broad)	Install	Succeeded
✓ 17 April 2026 12:51:00	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.150.0) - Current Channel (Broad)	Install	Succeeded
✓ 17 April 2026 15:22:08	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.152.0) - Current Channel (Broad)	Install	Succeeded
✓ 20 April 2026 07:10:12	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.199.0) - Current Channel (Broad)	Install	Succeeded
✓ 20 April 2026 16:09:03	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.206.0) - Current Channel (Broad)	Install	Succeeded
✓ 22 April 2026 09:45:46	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.240.0) - Current Channel (Broad)	Install	Succeeded
✓ 23 April 2026 07:38:39	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.257.0) - Current Channel (Broad)	Install	Succeeded
✓ 24 April 2026 10:33:54	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.272.0) - Current Channel (Broad)	Install	Succeeded
✓ 28 April 2026 10:09:06	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.340.0) - Current Channel (Broad)	Install	Succeeded
✓ 29 April 2026 08:53:58	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.354.0) - Current Channel (Broad)	Install	Succeeded
✓ 29 April 2026 15:26:57	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.357.0) - Current Channel (Broad)	Install	Succeeded
✓ 30 April 2026 09:51:35	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.367.0) - Current Channel (Broad)	Install	Succeeded
✓ 04 May 2026 09:54:36	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.441.0) - Current Channel (Broad)	Install	Succeeded
✓ 05 May 2026 11:39:57	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.457.0) - Current Channel (Broad)	Install	Succeeded
✓ 07 May 2026 07:39:21	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.490.0) - Current Channel (Broad)	Install	Succeeded
✓ 08 May 2026 08:59:26	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.508.0) - Current Channel (Broad)	Install	Succeeded
✓ 12 May 2026 06:55:05	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.573.0) - Current Channel (Broad)	Install	Succeeded
✓ 14 May 2026 08:18:22	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.608.0) - Current Channel (Broad)	Install	Succeeded
✓ 14 May 2026 08:58:10	9NKRJ3SJ9SDG-Microsoft.WindowsAppRuntime.1.8	Install	Succeeded
✓ 14 May 2026 08:58:10	9PLJQ12FQ3CV-MicrosoftCorporationII.WinAppRuntime.Main.1.8	Install	Succeeded

✓ 14 May 2026 08:58:10	9NKRJ3SJ9SDG-Microsoft.WindowsAppRuntime.1.8	Install	Succeeded
✓ 14 May 2026 13:44:36	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.612.0) - Current Channel (Broad)	Install	Succeeded
✓ 15 May 2026 09:03:44	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.627.0) - Current Channel (Broad)	Install	Succeeded
✓ 18 May 2026 08:02:10	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.675.0) - Current Channel (Broad)	Install	Succeeded
✓ 18 May 2026 14:35:05	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.680.0) - Current Channel (Broad)	Install	Succeeded
✓ 19 May 2026 15:05:11	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.449.696.0) - Current Channel (Broad)	Install	Succeeded
✓ 20 May 2026 08:11:54	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.6.0) - Current Channel (Broad)	Install	Succeeded
✓ 21 May 2026 09:06:24	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.26040.7) - Current Channel (Broad)	Install	Succeeded
✓ 21 May 2026 09:16:36	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.26.0) - Current Channel (Broad)	Install	Succeeded
✓ 21 May 2026 14:05:18	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.29.0) - Current Channel (Broad)	Install	Succeeded
✓ 22 May 2026 07:37:47	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.40.0) - Current Channel (Broad)	Install	Succeeded
✓ 22 May 2026 16:43:48	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.45.0) - Current Channel (Broad)	Install	Succeeded
✓ 26 May 2026 09:28:08	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.111.0) - Current Channel (Broad)	Install	Succeeded
✓ 26 May 2026 12:11:19	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.111.0) - Current Channel (Broad)	Install	Succeeded
✓ 26 May 2026 12:11:19	2026-05 .NET Framework Security Update (KB5087051)	Install	Succeeded
✓ 26 May 2026 12:21:22	2026-05 Security Update (KB5087539) (26100.32860)	Install	Succeeded
✓ 26 May 2026 12:22:50	Windows Malicious Software Removal Tool x64 - v5.141 (KB890830)	Install	Succeeded
✓ 26 May 2026 12:54:02	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.113.0) - Current Channel (Broad)	Install	Succeeded
✓ 27 May 2026 08:40:41	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.125.0) - Current Channel (Broad)	Install	Succeeded
✓ 28 May 2026 08:25:34	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.140.0) - Current Channel (Broad)	Install	Succeeded
✓ 02 June 2026 08:14:18	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.226.0) - Current Channel (Broad)	Install	Succeeded
✓ 02 June 2026 13:09:51	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.230.0) - Current Channel (Broad)	Install	Succeeded
✓ 08 June 2026 15:06:35	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.451.328.0) - Current Channel (Broad)	Install	Succeeded
✓ 10 June 2026 11:24:24	9PLUQ12FQ3CV-MicrosoftCorporationII.WinAppRuntime.Main.1.8	Install	Succeeded

✓ 10 June 2026 11:24:24	9NKRJ3SJ9SDG-Microsoft.WindowsAppRuntime.1.8	Install	Succeeded
✓ 10 June 2026 11:29:12	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.23.0) - Current Channel (Broad)	Install	Succeeded
✓ 11 June 2026 14:08:41	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.26050.15) - Current Channel (Broad)	Install	Succeeded
✓ 11 June 2026 14:18:56	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.44.0) - Current Channel (Broad)	Install	Succeeded
✓ 16 June 2026 11:58:50	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.121.0) - Current Channel (Broad)	Install	Succeeded
✓ 19 June 2026 14:16:22	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.178.0) - Current Channel (Broad)	Install	Succeeded
✓ 23 June 2026 09:56:56	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.240.0) - Current Channel (Broad)	Install	Succeeded
✓ 25 June 2026 14:07:00	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.276.0) - Current Channel (Broad)	Install	Succeeded
✓ 25 June 2026 15:00:34	Windows Malicious Software Removal Tool x64 - v5.142 (KB890830)	Install	Succeeded
✓ 25 June 2026 15:00:35	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.276.0) - Current Channel (Broad)	Install	Succeeded
✓ 25 June 2026 18:23:29	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.278.0) - Current Channel (Broad)	Install	Succeeded
✓ 25 June 2026 18:24:53	2026-06 Security Update (KB5094125) (26100.32995)	Install	Succeeded
✓ 26 June 2026 08:12:10	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.287.0) - Current Channel (Broad)	Install	Succeeded
✓ 29 June 2026 12:16:06	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.339.0) - Current Channel (Broad)	Install	Succeeded
✓ 29 June 2026 13:33:32	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.340.0) - Current Channel (Broad)	Install	Succeeded
✓ 01 July 2026 07:46:33	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.370.0) - Current Channel (Broad)	Install	Succeeded
✓ 01 July 2026 15:34:56	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.374.0) - Current Channel (Broad)	Install	Succeeded
✓ 07 July 2026 10:41:03	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.453.463.0) - Current Channel (Broad)	Install	Succeeded
✓ 08 July 2026 12:48:22	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.39.0) - Current Channel (Broad)	Install	Succeeded
✓ 09 July 2026 08:04:37	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.26060.3008) - Current Channel (Broad)	Install	Succeeded
✓ 09 July 2026 08:14:52	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.50.0) - Current Channel (Broad)	Install	Succeeded
✓ 09 July 2026 15:17:02	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.54.0) - Current Channel (Broad)	Install	Succeeded
✓ 10 July 2026 13:19:57	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.70.0) - Current Channel (Broad)	Install	Succeeded
✓ 13 July 2026 09:09:34	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.116.0) - Current Channel (Broad)	Install	Succeeded

✓	15 July 2026 17:20:27	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.159.0) - Current Channel (Broad)	Install	Succeeded
✓	16 July 2026 08:37:25	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.166.0) - Current Channel (Broad)	Install	Succeeded
✓	16 July 2026 17:25:32	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.172.0) - Current Channel (Broad)	Install	Succeeded
✓	17 July 2026 07:37:04	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.181.0) - Current Channel (Broad)	Install	Succeeded
✓	17 July 2026 12:21:21	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	17 July 2026 12:21:21	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	20 July 2026 12:47:42	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.235.0) - Current Channel (Broad)	Install	Succeeded
✓	20 July 2026 12:52:42	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	20 July 2026 12:52:42	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	20 July 2026 12:52:56	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	20 July 2026 12:52:56	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	21 July 2026 07:47:16	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	21 July 2026 07:47:16	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	21 July 2026 07:54:02	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.249.0) - Current Channel (Broad)	Install	Succeeded
✓	22 July 2026 13:18:43	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.269.0) - Current Channel (Broad)	Install	Succeeded
✓	23 July 2026 07:18:54	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.279.0) - Current Channel (Broad)	Install	Succeeded
✓	27 July 2026 07:29:27	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	27 July 2026 07:29:27	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	27 July 2026 07:30:52	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	27 July 2026 07:30:52	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	27 July 2026 07:31:11	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	27 July 2026 07:31:11	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	27 July 2026 07:32:12	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.368.0) - Current Channel (Broad)	Install	Succeeded
✓	28 July 2026 07:54:00	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.388.0) - Current Channel (Broad)	Install	Succeeded

✓ 29 July 2026 08:44:49	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 29 July 2026 08:44:49	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 29 July 2026 08:45:32	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 29 July 2026 08:45:32	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 29 July 2026 08:46:01	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 29 July 2026 08:46:02	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 29 July 2026 08:51:25	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.455.406.0) - Current Channel (Broad)	Install	Succeeded
✓ 05 August 2026 12:27:45	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.11.0) - Current Channel (Broad)	Install	Succeeded
✓ 07 August 2026 14:03:48	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.26070.9) - Current Channel (Broad)	Install	Succeeded
✓ 08 August 2026 15:26:01	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.65.0) - Current Channel (Broad)	Install	Succeeded
✓ 09 August 2026 07:53:03	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.75.0) - Current Channel (Broad)	Install	Succeeded
✓ 09 August 2026 08:02:24	2026-07 Security Update (KB5099536) (26100.33158)	Install	Succeeded
✓ 09 August 2026 08:03:27	2026-07 .NET Framework Security Update (KB5100998)	Install	Succeeded
✓ 09 August 2026 08:04:50	Windows Malicious Software Removal Tool x64 - v5.143 (KB890830)	Install	Succeeded
✓ 09 August 2026 08:04:51	Update for Windows Security platform - KB5007651 (Version 10.0.29628.1000)	Install	Succeeded
✓ 10 August 2026 02:42:06	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.87.0) - Current Channel (Broad)	Install	Succeeded
✓ 10 August 2026 06:57:32	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.87.0) - Current Channel (Broad)	Install	Succeeded
✓ 10 August 2026 06:57:59	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.90.0) - Current Channel (Broad)	Install	Succeeded
✓ 17 August 2026 16:09:38	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 17 August 2026 16:18:22	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.209.0) - Current Channel (Broad)	Install	Succeeded
✓ 17 August 2026 16:21:51	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 17 August 2026 16:21:51	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 17 August 2026 16:22:20	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 17 August 2026 16:22:20	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded

✓ 17 August 2026 17:10:49	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.209.0) - Current Channel (Broad)	Install	Succeeded
✓ 17 August 2026 17:16:59	2026-08 .NET Framework Security Update (KB5120708)	Install	Succeeded
✓ 17 August 2026 17:27:21	2026-08 Security Update (KB5120233) (26100.33296)	Install	Succeeded
✓ 17 August 2026 17:29:26	Windows Malicious Software Removal Tool x64 - v5.144 (KB890830)	Install	Succeeded
✓ 18 August 2026 02:25:53	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.217.0) - Current Channel (Broad)	Install	Succeeded
✓ 18 August 2026 09:25:01	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.222.0) - Current Channel (Broad)	Install	Succeeded
✓ 18 August 2026 09:38:25	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.222.0) - Current Channel (Broad)	Install	Succeeded
✓ 19 August 2026 07:46:47	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.239.0) - Current Channel (Broad)	Install	Succeeded
✓ 21 August 2026 09:51:25	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.269.0) - Current Channel (Broad)	Install	Succeeded
✓ 21 August 2026 09:55:18	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 21 August 2026 09:55:38	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 21 August 2026 14:26:03	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 27 August 2026 12:51:44	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 27 August 2026 12:57:01	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 27 August 2026 12:57:19	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 27 August 2026 12:57:36	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.362.0) - Current Channel (Broad)	Install	Succeeded
✓ 28 August 2026 07:30:50	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.375.0) - Current Channel (Broad)	Install	Succeeded
✓ 31 August 2026 09:58:56	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 31 August 2026 10:03:24	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.457.425.0) - Current Channel (Broad)	Install	Succeeded
✓ 07 September 2026 09:31:21	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.91.0) - Current Channel (Broad)	Install	Succeeded
✓ 07 September 2026 09:34:55	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 07 September 2026 09:40:58	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓ 07 September 2026 09:41:03	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.26080.3) - Current Channel (Broad)	Install	Succeeded
✓ 07 September 2026 09:42:43	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded

✓	07 September 2026 11:58:50	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.93.0) - Current Channel (Broad)	Install	Succeeded
✓	07 September 2026 12:04:22	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.26080.3) - Current Channel (Broad)	Install	Succeeded
✓	08 September 2026 08:01:41	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.103.0) - Current Channel (Broad)	Install	Succeeded
✓	08 September 2026 13:27:49	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.111.0) - Current Channel (Broad)	Install	Succeeded
✓	09 September 2026 08:05:00	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	09 September 2026 08:12:47	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.123.0) - Current Channel (Broad)	Install	Succeeded
✓	09 September 2026 09:42:59	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.124.0) - Current Channel (Broad)	Install	Succeeded
✓	15 September 2026 14:28:17	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.221.0) - Current Channel (Broad)	Install	Succeeded
✓	15 September 2026 14:30:49	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	15 September 2026 14:55:04	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.221.0) - Current Channel (Broad)	Install	Succeeded
✓	15 September 2026 15:16:08	2026-09 Security Update (KB5122871) (26100.33438)	Install	Succeeded
✓	17 September 2026 10:08:52	Windows Malicious Software Removal Tool x64 - v5.145 (KB890830)	Install	Succeeded
✓	17 September 2026 10:10:18	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	17 September 2026 10:10:19	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	17 September 2026 10:10:36	2026-09 .NET Framework Security Update (KB5126052)	Install	Succeeded
✓	17 September 2026 10:14:33	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.250.0) - Current Channel (Broad)	Install	Succeeded
✓	18 September 2026 04:13:38	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.26080.4) - Current Channel (Broad)	Install	Succeeded
✓	18 September 2026 04:23:48	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.459.263.0) - Current Channel (Broad)	Install	Succeeded
✓	21 September 2026 10:16:06	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	21 September 2026 10:16:06	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	21 September 2026 10:16:06	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	21 September 2026 10:26:30	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	21 September 2026 10:26:30	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
✓	21 September 2026 10:26:30	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded

 21 September 2026 10:26:52	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
 21 September 2026 10:26:52	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	Install	Succeeded
 21 September 2026 10:26:52	9NRZT3Q9R3DL-Microsoft.WindowsAppRuntime.2	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]



Windows Server 2025
Datacenter

General

Installed Programs	15 Installed Programs
Event Logs	14 Event Logs
Environment Variables	23 Environment Variables
Scheduled Tasks	6 Scheduled Tasks

.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	

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.

23 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
 %IDENTITY_ENDPOINT%	<SYSTEM>	http://localhost:40342/metadata/identity/oauth2/token
 %IMDS_ENDPOINT%	<SYSTEM>	http://localhost:40342
 %NUMBER_OF_PROCESSORS%	<SYSTEM>	2
 %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\AzureConnectedMachineAgent\ C:\WINDOWS\System32
 %PATHEXT%	<SYSTEM>	.COM .EXE .BAT .CMD .VBS .VBE

		.JS .JSE .WSF .WSH .MSC
 %PROCESSOR_ARCHITECTURE%	<SYSTEM>	AMD64
 %PROCESSOR_IDENTIFIER%	<SYSTEM>	Intel64 Family 6 Model 141 Stepping 1, GenuineIntel
 %PROCESSOR_LEVEL%	<SYSTEM>	6
 %PROCESSOR_REVISION%	<SYSTEM>	8d01
 %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
 %SystemDrive%	<SYSTEM>	C:
 %SystemRoot%	<SYSTEM>	C:\WINDOWS
 %TEMP%	<SYSTEM>	C:\WINDOWS\TEMP
 %TMP%	<SYSTEM>	C:\WINDOWS\TEMP
 %USERNAME%	<SYSTEM>	SYSTEM
 %windir%	<SYSTEM>	C:\WINDOWS

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.

14 Event Logs

Name	Type	Maximum File Size	Retention Policy
 Active Directory Web Services	Administrative	1,028 KB	Overwrite events as needed
 Application	Administrative	20,480 KB	Overwrite events as needed
 DFS Replication	Administrative	15,168 KB	Overwrite events as needed
 Directory Service	Administrative	1,028 KB	Overwrite events as needed
 DNS Server	Administrative	102,400 KB	Overwrite events as needed
 ECMA2Host	Administrative	102,400 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	131,072 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
 WindowsAdminCenter	Administrative	102,400 KB	Overwrite events as needed

Active Directory Web Services

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	Active Directory Web Services
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\Active Directory Web Services.evtx
Log Type	Administrative
File Size	1 MB
Record Count	1,053

File Access

Created	08 April 2026 14:28:13
Last Accessed	21 September 2026 11:24:47
Last Modified	21 September 2026 11:24:47

Retention

Maximum File Size	1,028 KB
Retention Policy	Overwrite events as needed

Active Directory Web Services

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	21 September 2026 11:23:27	ADWS	1200	ADWS Instance Events	N/A
 Information	21 September 2026 11:22:28	ADWS	1004	ADWS Instance Events	N/A
 Error	21 September 2026 11:22:28	ADWS	1005	ADWS Startup Events	N/A
 Information	21 September 2026 11:22:27	ADWS	1200	ADWS Instance Events	N/A
 Information	21 September 2026 11:22:27	ADWS	1400	ADWS Instance Events	N/A
 Information	21 September 2026 11:22:27	ADWS	1008	ADWS Instance Events	N/A
 Information	21 September 2026 11:22:27	ADWS	1100	ADWS Startup Events	N/A
 Information	21 September 2026 11:22:27	ADWS	1000	ADWS Instance Events	N/A
 Information	21 September 2026 11:12:22	ADWS	1200	ADWS Instance Events	N/A
 Information	21 September 2026 11:11:22	ADWS	1004	ADWS Instance Events	N/A

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	4.07 MB
Record Count	4,299

File Access

Created	06 November 2024 19:58:46
Last Accessed	21 September 2026 11:25:31
Last Modified	21 September 2026 11:25:31

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	21 September 2026 11:25:44	Security-SPP	1003	None	N/A
 Information	21 September 2026 11:25:32	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:25:31	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:25:31	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:25:31	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:25:31	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:25:31	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:25:31	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:25:31	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:25:31	Windows Error Reporting	1001	None	NT AUTHORITY\SYSTEM

DFS Replication

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	DFS Replication
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\DFS Replication.evtx
Log Type	Administrative
File Size	1.07 MB
Record Count	1,364

File Access

Created	08 April 2026 14:28:13
Last Accessed	21 September 2026 11:24:47
Last Modified	21 September 2026 11:24:47

Retention

Maximum File Size	15,168 KB
Retention Policy	Overwrite events as needed

DFS Replication

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
 Error	21 September 2026 11:22:54	DFSR	4012	None	N/A
 Information	21 September 2026 11:22:54	DFSR	1210	None	N/A
 Information	21 September 2026 11:22:42	DFSR	1206	None	N/A
 Information	21 September 2026 11:22:29	DFSR	6102	None	N/A
 Information	21 September 2026 11:22:27	DFSR	1314	None	N/A
 Information	21 September 2026 11:22:27	DFSR	1004	None	N/A
 Information	21 September 2026 11:22:26	DFSR	1002	None	N/A
 Information	21 September 2026 11:21:59	DFSR	1006	None	N/A
 Error	21 September 2026 11:18:56	DFSR	4012	None	N/A
 Error	21 September 2026 11:11:56	DFSR	4012	None	N/A

Directory 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	Directory Service
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\Directory Service.evtx
Log Type	Administrative
File Size	1 MB
Record Count	2,236

File Access

Created	08 April 2026 14:28:13
Last Accessed	21 September 2026 11:24:47
Last Modified	21 September 2026 11:24:47

Retention

Maximum File Size	1,028 KB
Retention Policy	Overwrite events as needed

Directory Service

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	21 September 2026 11:24:42	ActiveDirectory_DomainService	2946	Security	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:22:56	ActiveDirectory_DomainService	1394	Security	NT AUTHORITY\ANONYMOUS LOGON
 Error	21 September 2026 11:22:42	ActiveDirectory_DomainService	1126	Global Catalog	NT AUTHORITY\ANONYMOUS LOGON
 Information	21 September 2026 11:22:26	ActiveDirectory_DomainService	1000	Security	NT AUTHORITY\ANONYMOUS LOGON
 Information	21 September 2026 11:22:16	ActiveDirectory_DomainService	2405	Security	NT AUTHORITY\ANONYMOUS LOGON
 Information	21 September 2026 11:22:16	ActiveDirectory_DomainService	2405	Security	NT AUTHORITY\ANONYMOUS LOGON
 Information	21 September 2026 11:22:16	ActiveDirectory_DomainService	2405	Security	NT AUTHORITY\ANONYMOUS LOGON
 Information	21 September 2026 11:22:16	ActiveDirectory_DomainService	2120	Security	NT AUTHORITY\ANONYMOUS LOGON
 Information	21 September 2026 11:22:16	ActiveDirectory_DomainService	2172	Security	NT AUTHORITY\ANONYMOUS LOGON
 Information	21 September 2026 11:22:16	ActiveDirectory_DomainService	2168	Security	NT AUTHORITY\ANONYMOUS LOGON

DNS Server

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	DNS Server
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\DNS Server.evtx
Log Type	Administrative
File Size	1.07 MB
Record Count	1,156

File Access

Created	08 April 2026 14:37:46
Last Accessed	21 September 2026 11:24:47
Last Modified	21 September 2026 11:24:47

Retention

Maximum File Size	102,400 KB
Retention Policy	Overwrite events as needed

DNS Server

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	21 September 2026 11:22:57	DNS-Server-Service	4	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:22:56	DNS-Server-Service	2	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:22:56	DNS-Server-Service	769	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:22:56	DNS-Server-Service	769	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:22:56	DNS-Server-Service	769	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:22:56	DNS-Server-Service	769	None	NT AUTHORITY\SYSTEM
 Warning	21 September 2026 11:22:32	DNS-Server-Service	4013	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:22:27	DNS-Server-Service	7693	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:21:59	DNS-Server-Service	3	None	NT AUTHORITY\SYSTEM
 Information	21 September 2026 11:11:51	DNS-Server-Service	4	None	NT AUTHORITY\SYSTEM

ECMA2Host

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	ECMA2Host
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\ECMA2Host.evtx
Log Type	Administrative
File Size	68 KB
Record Count	123

File Access

Created	13 April 2026 17:20:27
Last Accessed	21 September 2026 11:24:47
Last Modified	21 September 2026 11:24:47

Retention

Maximum File Size	102,400 KB
Retention Policy	Overwrite events as needed

ECMA2Host

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	21 September 2026 11:22:27	ECMA2Host.MainDomain	1	None	N/A
 Information	21 September 2026 11:11:22	ECMA2Host.MainDomain	1	None	N/A
 Information	18 September 2026 05:02:57	ECMA2Host.MainDomain	1	None	N/A
 Information	18 September 2026 05:01:08	ECMA2Host.MainDomain	1	None	N/A
 Information	17 September 2026 11:03:54	ECMA2Host.MainDomain	1	None	N/A
 Information	15 September 2026 15:16:58	ECMA2Host.MainDomain	1	None	N/A
 Information	09 September 2026 10:32:08	ECMA2Host.MainDomain	1	None	N/A
 Information	09 September 2026 09:02:15	ECMA2Host.MainDomain	1	None	N/A
 Information	08 September 2026 14:17:10	ECMA2Host.MainDomain	1	None	N/A
 Information	08 September 2026 14:10:14	ECMA2Host.MainDomain	1	None	N/A

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	06 November 2024 19:58:46
Last Accessed	06 November 2024 19:59:32
Last Modified	06 November 2024 19:59:32

 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	06 November 2024 19:58:46
Last Accessed	06 November 2024 19:59:32
Last Modified	06 November 2024 19:59:32

 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	89.07 MB
Record Count	108,480

File Access

Created	06 November 2024 19:58:46
Last Accessed	21 September 2026 11:25:49
Last Modified	21 September 2026 11:25:49

Retention

Maximum File Size	131,072 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	21 September 2026 11:25:54	Security-Auditing	5061	System Integrity	N/A
 Success Audit	21 September 2026 11:25:54	Security-Auditing	5058	System Integrity	N/A
 Success Audit	21 September 2026 11:25:43	Security-Auditing	4634	System Integrity	N/A
 Success Audit	21 September 2026 11:25:43	Security-Auditing	5061	System Integrity	N/A
 Success Audit	21 September 2026 11:25:43	Security-Auditing	5058	System Integrity	N/A
 Success Audit	21 September 2026 11:25:43	Security-Auditing	5061	System Integrity	N/A
 Success Audit	21 September 2026 11:25:43	Security-Auditing	5058	System Integrity	N/A
 Success Audit	21 September 2026 11:25:38	Security-Auditing	5061	System Integrity	N/A
 Success Audit	21 September 2026 11:25:38	Security-Auditing	5058	System Integrity	N/A
 Success Audit	21 September 2026 11:25:33	Security-Auditing	5061	System Integrity	N/A

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	68 KB
Record Count	143

File Access

Created	06 November 2024 19:58:46
Last Accessed	18 September 2026 05:05:15
Last Modified	18 September 2026 05:05:15

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	18 September 2026 05:03:12	Servicing	2	None	NT AUTHORITY\SYSTEM
 Information	18 September 2026 05:03:10	Servicing	2	None	NT AUTHORITY\SYSTEM
 Information	18 September 2026 05:03:10	Servicing	2	None	NT AUTHORITY\SYSTEM
 Information	17 September 2026 11:10:35	Servicing	4	None	NT AUTHORITY\SYSTEM
 Information	17 September 2026 11:09:53	Servicing	1	None	NT AUTHORITY\SYSTEM
 Information	17 September 2026 11:09:49	Servicing	2	None	NT AUTHORITY\SYSTEM
 Information	17 September 2026 11:09:10	Servicing	1	None	NT AUTHORITY\SYSTEM
 Information	15 September 2026 16:16:36	Servicing	3	None	NT AUTHORITY\SYSTEM
 Information	15 September 2026 16:16:17	Servicing	1	None	NT AUTHORITY\SYSTEM
 Information	15 September 2026 16:16:03	Servicing	4	None	NT AUTHORITY\SYSTEM

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	4.07 MB
Record Count	10,232

File Access

Created	06 November 2024 19:58:46
Last Accessed	21 September 2026 11:25:50
Last Modified	21 September 2026 11:25:50

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	21 September 2026 11:25:31	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:30	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:30	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:30	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:29	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:29	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:28	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:26	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:16	Service Control Manager	7036	None	N/A
 Information	21 September 2026 11:25:12	Service Control Manager	7036	None	N/A

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	15 MB
Record Count	7,272

File Access

Created	06 November 2024 19:58:46
Last Accessed	21 September 2026 11:25:46
Last Modified	21 September 2026 11:25:46

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	21 September 2026 11:25:43	PowerShell	800	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:36	PowerShell	400	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:36	PowerShell	600	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:36	PowerShell	600	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:36	PowerShell	600	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:36	PowerShell	600	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:36	PowerShell	600	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:36	PowerShell	600	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:20	PowerShell	403	Pipeline Execution Details	N/A
 Information	21 September 2026 11:25:20	PowerShell	400	Pipeline Execution Details	N/A

WindowsAdminCenter

The event logging service records events from various sources and stores them in a single collection called an event log.

Event Log Settings

Name	WindowsAdminCenter
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\WindowsAdminCenter.evtx
Log Type	Administrative
File Size	4.07 MB
Record Count	3,164

File Access

Created	17 August 2026 18:12:01
Last Accessed	21 September 2026 11:24:47
Last Modified	21 September 2026 11:24:47

Retention

Maximum File Size	102,400 KB
Retention Policy	Overwrite events as needed

WindowsAdminCenter

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	21 September 2026 11:23:30	Core	102	None	N/A
 Information	21 September 2026 11:22:31	WinREST	202	None	N/A
 Information	21 September 2026 11:22:31	WinStream	202	None	N/A
 Information	21 September 2026 11:22:30	WinREST	202	None	N/A
 Information	21 September 2026 11:22:30	WinREST	202	None	N/A
 Information	21 September 2026 11:22:30	WinREST	202	None	N/A
 Information	21 September 2026 11:22:30	WinREST	202	None	N/A
 Information	21 September 2026 11:22:30	WinREST	202	None	N/A
 Information	21 September 2026 11:22:30	WinREST	202	None	N/A
 Information	21 September 2026 11:22:30	WinREST	202	None	N/A

Installed Software

Provides information about the programs installed on this Windows machine.

15 Installed Programs

Name	Publisher	Platform	Version	Installation Date
 Azure Connected Machine Agent	Microsoft Corporation	64 bit	1.67.03504.3207	17 August 2026
 Google Chrome	Google LLC	32 bit	153.0.8010.52	18 September 2026
 GPO Comparison Tool	CENTREL Solutions	64 bit	18.0.15	22 April 2026
 Microsoft Azure AD Connect Agent Updater	Microsoft Corporation	64 bit	1.5.4846.0	29 June 2026
 Microsoft Azure AD Connect Provisioning Agent	Microsoft Corporation	64 bit	1.1.2108.0	13 April 2026
 Microsoft Edge	Microsoft Corporation	32 bit	153.0.4234.32	15 September 2026
 Microsoft Edge WebView2 Runtime	Microsoft Corporation	32 bit	153.0.4234.32	17 September 2026
 Microsoft Entra Provisioning Agent Package	Microsoft Corporation	64 bit	1.1.2108.0	13 April 2026
 Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.40.33816	Microsoft Corporation	32 bit	14.40.33816.0	08 April 2026
 Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.40.33816	Microsoft Corporation	32 bit	14.40.33816.0	08 April 2026
 Microsoft Windows Application Compatibility Fix Database		64 bit		07 September 2026
 VMware Tools	Broadcom Inc.	64 bit	13.1.5.0	21 September 2026
 Windows Admin Center (v2)	Microsoft Corporation	64 bit	2.4.1.2	18 August 2026
 XIA Configuration Client	CENTREL Solutions	64 bit	18.1.6	15 September 2026
 XIA Configuration Express	CENTREL Solutions	64 bit	18.1.6	21 September 2026

Internet Settings

This section provides information about the Internet Settings for the machine including the system level proxy settings.

 Internet Settings

Internet Explorer Version	11.32860.26100.0
---------------------------	------------------

 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.

 ODBC Configuration

Drivers	18
Data Sources	0

ODBC Drivers

An ODBC driver provides the ability to translate commands between an ODBC client applications and the backend data source.

18 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
 SQL Server	x86	3.50	10.0.26100.3624	SQLSRV32.dll
 SQL Server	x64	3.50	10.0.26100.3624	SQLSRV32.dll

ODBC 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.

 **0 ODBC Data Sources**

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-QJ69T
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	21 September 2026 11:22:10
Install Date	08 April 2026 11:19:54
Locale	0809
MUI Languages	en-US
Operating System Language	1033
Serial Number	00491-60000-08052-AA587
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32

Naming and Role

Domain	centrelsolutionsdemo.int
Domain Role	Domain Controller (PDC emulator)
NetBIOS Name	CSDEMO-DC01
Fully Qualified Domain Name	csdemo-dc01.centrelsolutionsdemo.int

Timezone

Time Zone Name	(UTC+00:00) Dublin, Edinburgh, Lisbon, London
Daylight In Effect	True
Time Zone Bias	0

Registry

Registry Size (Current)	148
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 5.1.26100.33438
Runtime Version	4.0.30319.42000
Compatible Versions	1.0 2.0 3.0 4.0 5.0 5.1.26100.33438
Machine Execution Policy	Remote Signed
Machine Execution Policy Source	Local

3 Permissions

Account Name	Type	Rights
 BUILTIN\Administrators	Allow	Full Control (All Operations)
 NT AUTHORITY\INTERACTIVE	Allow	Full Control (All Operations)
 BUILTIN\Remote Management Users	Allow	Full Control (All Operations)

3 Audit Rules

Account Name	Type	Rights
 Everyone	Audit	Full Control (All Operations)
 Everyone	Audit	Execute (Invoke), Write (Put, Delete, Create)

Registry

The Windows registry is a hierarchical database that contains configuration data for the operating system, applications, and services.

 **0 Registry Keys**

There are no registry keys documented for this Windows machine.

 **0 Registry Values**

There are no registry values documented for this Windows machine.

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	Available
☒ 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	Installed
☐ 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	Installed
☐ Enhanced Storage	Available
☐ Failover Clustering	Available
☐ Fax Server	Available
☒ File and Storage Services	Installed
☒ File and iSCSI Services	Installed
☐ BranchCache for Network Files	Available
☐ Data Deduplication	Available
☒ DFS Namespaces	Installed
☒ DFS Replication	Installed
☒ File Server	Installed
☐ File Server Resource Manager	Available
☐ File Server VSS Agent Service	Available
☒ iSCSI Target Server	Installed
☐ 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	Installed
☒ Active Directory Administrative Center	Installed
☒ AD DS Snap-Ins and Command-Line Tools	Installed
☐ AD LDS Snap-Ins and Command-Line Tools	Available
☐ DHCP Server Tools	Available
☒ DNS Server Tools	Installed
☐ 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
☐ Sysmon	Available
☒ System Data Archiver	Installed
☐ System Insights	Available
☒ Telnet Client	Installed
☐ TFTP Client	Available
☐ VM Shielding Tools for Fabric Management	Available
☐ Volume Activation Services	Available
☐ Web Server (IIS)	Available
☐ FTP Server	Available
☐ FTP Extensibility	Available
☐ FTP Service	Available
☐ Management Tools	Available
☐ IIS 6 Management Compatibility	Available
☐ IIS 6 Metabase Compatibility	Available
☐ IIS 6 Scripting Tools	Available
☐ IIS 6 WMI Compatibility	Available
☐ IIS Management Console	Available
☐ IIS Management Scripts and Tools	Available

☐ Management Service	Available
☐ Web Server	Available
☐ Application Development	Available
☐ .NET Extensibility 3.5	Available
☐ .NET Extensibility 4.8	Available
☐ Application Initialization	Available
☐ ASP	Available
☐ ASP.NET 3.5	Available
☐ ASP.NET 4.8	Available
☐ CGI	Available
☐ ISAPI Extensions	Available
☐ ISAPI Filters	Available
☐ Server Side Includes	Available
☐ WebSocket Protocol	Available
☐ Common HTTP Features	Available
☐ Default Document	Available
☐ Directory Browsing	Available
☐ HTTP Errors	Available
☐ HTTP Redirection	Available
☐ Static Content	Available
☐ WebDAV Publishing	Available
☐ Health and Diagnostics	Available
☐ Custom Logging	Available
☐ HTTP Logging	Available
☐ Logging Tools	Available
☐ ODBC Logging	Available
☐ Request Monitor	Available
☐ Tracing	Available
☐ Performance	Available
☐ Dynamic Content Compression	Available
☐ Static Content Compression	Available
☐ Security	Available
☐ 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	Available
☐ URL Authorization	Available
☐ Windows Authentication	Available
☐ 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	Available
☐ .NET Environment 3.5	Available
☐ Configuration APIs	Available
☐ Process Model	Available
☐ Windows Search Service	Available
☒ Windows Server Backup	Installed
☐ 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

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.

6 Scheduled Tasks

Name	Triggers	Account Name
 azcmagent	At 01:15 every day	NT AUTHORITY\SYSTEM
 CreateExplorerShellUnelevatedTask	When the task is created or modified	CSDEMO\Administrator
 GoogleUpdaterTaskSystem152.0.7933.0{560858BF-9381-4356-A4A1-F6958A00D7B2}	Multiple triggers defined	NT AUTHORITY\SYSTEM
 MicrosoftEdgeUpdateTaskMachineCore{0180DB29-C278-4BBC-BD83-2AD720678EF4}	Multiple triggers defined	NT AUTHORITY\SYSTEM
 MicrosoftEdgeUpdateTaskMachineUA{0788BB83-9448-4452-B945-D7FABFF6FCF7}	At 11:24 every day	NT AUTHORITY\SYSTEM
 WindowsAdminCenterUpdater	No triggers defined	NT AUTHORITY\SYSTEM

azcmagent

Scheduled tasks can be used to schedule commands, programs, or scripts to run at specific times.

General

Name	azcmagent
Task Path	\
Author	CSDEMO\CSDEMO-DC01\$
Enabled	True
Date	17 August 2026 17:22:55
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	False

Settings

Allow Task To Be Run On Demand	True
Run After Missed Scheduled Start	False
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	True
Stop Task When Going On Batteries	True
Wake Computer To Run Task	False
Network Requirement	None

Execute Action

Command	C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe
Arguments	-File "C:\Program Files\AzureConnectedMachineAgent\azcmagent_check_updates.ps1"
Working Directory	

On specified schedule

Summary	At 01:15 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

CreateExplorerShellUnelevatedTask

Scheduled tasks can be used to schedule commands, programs, or scripts to run at specific times.

General

Name	CreateExplorerShellUnelevatedTask
Task Path	\
Author	ExplorerShellUnelevated
Enabled	True
Hidden	False
Version	Windows ® 7, Windows Server™ 2008 R2

Security

Account Name	CSDEMO\Administrator
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:\WINDOWS\Explorer.EXE
Arguments	/NoUACCheck
Working Directory	

 When the task is created or modified

Summary	When the task is created or modified
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

GoogleUpdaterTaskSystem152.0.7933.0{560858BF-9381-4356-A4A1-F6958A00D7B2}

GoogleUpdater Task System 152.0.7933.0

General

Name	GoogleUpdaterTaskSystem152.0.7933.0{560858BF-9381-4356-A4A1-F6958A00D7B2}
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\152.0.7933.0\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 18:20 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{0180DB29-C278-4BBC-BD83-2AD720678EF4}

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{0180DB29-C278-4BBC-BD83-2AD720678EF4}
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	Run a new instance in parallel

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 11:54 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{0788BB83-9448-4452-B945-D7FABFF6FCF7}

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{0788BB83-9448-4452-B945-D7FABFF6FCF7}
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 11:24 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

WindowsAdminCenterUpdater

Scheduled tasks can be used to schedule commands, programs, or scripts to run at specific times.

General

Name	WindowsAdminCenterUpdater
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	False
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	True
Stop Task When Going On Batteries	True
Wake Computer To Run Task	False
Network Requirement	None

 Execute Action

Command	C:\ProgramData\WindowsAdminCenter\Updater\WindowsAdminCenterUpdater.exe
Arguments	
Working Directory	

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

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	10.0.26100.32860

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

261 Windows Services

Display Name	Start Mode	Account Name
 Active Directory Domain Services	Automatic	LocalSystem
 Active Directory Web Services	Automatic	LocalSystem
 ActiveX Installer (AxInstSV)	Manual	LocalSystem
 App Readiness	Manual	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)	Automatic (Trigger Start)	LocalSystem
 Auto Time Zone Updater	Disabled	NT AUTHORITY\LocalService
 AVCTP service	Manual (Trigger Start)	NT AUTHORITY\LocalService
 Azure Arc Proxy	Automatic (Delayed Start)	NT AUTHORITY\NetworkService
 Azure Hybrid Instance Metadata Service	Automatic (Delayed Start)	NT SERVICE\himds
 Background Intelligent Transfer Service	Automatic (Delayed Start)	LocalSystem
 Background Tasks Infrastructure Service	Automatic	LocalSystem
 Base Filtering Engine	Automatic	NT AUTHORITY\LocalService
 Block Level Backup Engine Service	Manual	localSystem

 Bluetooth Audio Gateway Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
 Bluetooth Support Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
 Bluetooth User Support Service_84845	Manual (Trigger Start)	
 Capability Access Manager Service	Automatic	LocalSystem
 CaptureService_84845	Manual	
 Certificate Propagation	Manual (Trigger Start)	LocalSystem
 Client License Service (ClipSVC)	Manual (Trigger Start)	LocalSystem
 Clipboard User Service_84845	Automatic	
 Cloud Backup and Restore Service_84845	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_84845	Automatic	
 Connected User Experiences and Telemetry	Automatic	LocalSystem
 ConsentUX User Service_84845	Manual	
 Contact Data_84845	Manual	
 CoreMessaging	Automatic	NT AUTHORITY\LocalService
 Credential Manager	Manual	LocalSystem
 CredentialEnrollmentManagerUserSvc_84845	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_84845	Manual	
 DevicePicker_84845	Manual	
 DevicesFlow_84845	Manual	
 DevQuery Background Discovery Broker	Manual (Trigger Start)	LocalSystem
 DFS Namespace	Automatic	LocalSystem
 DFS Replication	Automatic	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 Enhancement Service	Manual (Trigger Start)	LocalSystem
 Display Policy Service	Automatic	NT AUTHORITY\LocalService

 Distributed Link Tracking Client	Manual	LocalSystem
 Distributed Transaction Coordinator	Automatic (Delayed Start)	NT AUTHORITY\NetworkService
 DNS Client	Automatic (Trigger Start)	NT AUTHORITY\NetworkService
 DNS Server	Automatic	LocalSystem
 Downloaded Maps Manager	Disabled	NT AUTHORITY\NetworkService
 DS Role Server	Manual	LocalSystem
 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
 File Replication	Disabled	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 (GoogleUpdaterInternalService152.0.7933.0)	Automatic	LocalSystem
 Google Updater Service (GoogleUpdaterService152.0.7933.0)	Automatic	LocalSystem
 GraphicsPerfSvc	Manual (Trigger Start)	LocalSystem
 Group Policy Client	Automatic (Trigger Start)	LocalSystem
 Guest Configuration Arc Service	Automatic (Delayed Start)	LocalSystem

 Guest Configuration Extension Service	Automatic (Delayed Start)	LocalSystem
 Hotpatch Monitoring Service	Manual	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	Automatic (Trigger Start)	LocalSystem
 Internet Connection Sharing (ICS)	Manual (Trigger Start)	LocalSystem
 Intersite Messaging	Automatic	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 Key Distribution Center	Automatic	LocalSystem
 Kerberos Local Key Distribution Center	Manual	LocalSystem

 KtmRm for Distributed Transaction Coordinator	Manual (Trigger Start)	NT AUTHORITY\NetworkService
 Language Experience Service	Manual	LocalSystem
 Link-Layer Topology Discovery Mapper	Manual	NT AUTHORITY\LocalService
 Local Session Manager	Automatic	LocalSystem
 McpManagementService	Manual	LocalSystem
 Microsoft Account Sign-in Assistant	Manual (Trigger Start)	LocalSystem
 Microsoft App-V Client	Disabled	LocalSystem
 Microsoft Azure AD Connect Agent Updater	Automatic (Delayed Start)	NT Authority\System
 Microsoft Azure AD Connect Provisioning Agent	Automatic (Delayed Start)	centrelsolutionsdemo.int\pGMSA_c2ca7496\$
 Microsoft Defender Antivirus Network Inspection Service	Manual	NT AUTHORITY\LocalService
 Microsoft Defender Antivirus Service	Automatic	LocalSystem
 Microsoft Defender Core Service	Automatic	LocalSystem
 Microsoft ECMA2Host	Automatic	NT AUTHORITY\NetworkService
 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 iSCSI Target Server	Automatic	localSystem
 Microsoft Key Distribution Service	Manual (Trigger Start)	LocalSystem
 Microsoft Passport	Manual (Trigger Start)	LocalSystem
 Microsoft Passport Container	Manual (Trigger Start)	NT AUTHORITY\LocalService

 Microsoft Software Shadow Copy Provider	Manual	LocalSystem
 Microsoft Storage Spaces SMP	Manual	NT AUTHORITY\NetworkService
 Microsoft Store Install Service	Manual	LocalSystem
 Natural Authentication	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
 Now Playing Session Manager Service_84845	Manual	
 Offline Files	Disabled	LocalSystem
 OpenSSH Authentication Agent	Disabled	LocalSystem
 OpenSSH SSH Server	Manual	LocalSystem
 Optimize drives	Manual	localSystem
 P9RdrService_84845	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_84845	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
 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_84845	Automatic	
 SysMain	Automatic	LocalSystem
 System Event Notification Service	Automatic	LocalSystem
 System Events Broker	Automatic (Trigger Start)	LocalSystem
 Task Scheduler	Automatic (Trigger Start)	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_84845	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_84845	Manual	
 User Data Storage_84845	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
 WaaSMedicSvc	Manual	LocalSystem
 WalletService	Manual	LocalSystem
 Warp JIT Service	Manual (Trigger Start)	NT Authority\LocalService
 Web Account Manager	Manual	LocalSystem
 Wi-Fi Direct Services Connection Manager Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
 Windows Admin Center	Automatic	NT Authority\NetworkService
 Windows Admin Center Account Management	Manual	LocalSystem
 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 Management Service	Manual	LocalSystem
 Windows Media Player Network Sharing Service	Manual	NT AUTHORITY\NetworkService
 Windows Modules Installer	Manual	localSystem
 Windows Push Notifications System Service	Automatic	LocalSystem
 Windows Push Notifications User Service_84845	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	Manual (Trigger Start)	LocalSystem
 WinHTTP Web Proxy Auto-Discovery Service	Manual	NT AUTHORITY\LocalService
 Wired AutoConfig	Manual	localSystem
 WLAN AutoConfig	Manual	LocalSystem
 WMI Performance Adapter	Manual	localSystem
 Work Folders	Manual	NT AUTHORITY\LocalService
 Workstation	Automatic	NT AUTHORITY\NetworkService
 WSAIFabricSvc	Automatic	NT AUTHORITY\LocalService
 Xbox Live Auth Manager	Manual	LocalSystem
 XIA Configuration Service	Automatic	CSDEMO\XiaClient
 ZTDNS Helper service	Manual	LocalSystem

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	Domain Controller (PDC emulator)
-------------	----------------------------------

Service Information

Start Mode	Automatic (Trigger Start)
Service State	Running

Global Settings

 MaxNegPhaseCorrection	172,800
 MaxPosPhaseCorrection	172,800
 VMIC Provider Status	Enabled

Client Settings

 Enabled	True
 Client Type	Domain Hierarchy (NT5DS)
 Special Poll Interval	1,024

Server Settings

 Enabled	True
 Announce Flags	Automatically determine whether to advertise reliable time service Automatically determine whether to advertise time service.

About XIA Configuration

XIA Configuration is an IT infrastructure audit and documentation tool that automates the process of collecting and documenting network configurations.