Windows Machine Report

XCS-2K22

CONTOSO FOODS

Date	02 September 2022 13:04:39
Author	TEST2022\sysadmin
Version	1.01
Product	XIA Configuration Server [14.1.7.0]

Table of Contents

Disclaimer

This document is for authorised use by the intended recipient(s) only. It may contain proprietary material, confidential information and/or be subject to legal privilege. It should not be copied, disclosed to, retained, or used by any other party.

Microsoft, Windows and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Windows Server Information

Provides general information for this item.

General Information

Name	XCS-2K22
Description	Windows Server 2022 server running XIA Configuration Server.
Primary Owner Name	Technical Services
Primary Owner Contact	technicalservices@contosofoods.com

System Information

Item Path	Demonstration Company > IT
Item ID	1026
Version ID	1.01
Check Out Status	Available

ProLiant DL360 G4

Custom Item Details

This is a demonstration Windows server running XIA Configuration Server.

Client Information

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

Item Identifiers

Primary Identifier	XCS-2K22
Secondary Identifier	VMware-56 4d 42 da e0 b5 8b 9e-c0 ea ef f4 59 bd 06 dd
Tertiary Identifier	
Environment Identifier	

Client Information

Client Machine Name	XCS-2K22
Client Identifier	7fa99657-d78d-466b-b246-03fac76de7dc
Client IP Address	192.168.131.246
Client Scan Date	02 September 2022 12:36 (today)
Client Service Username	TEST2022\sysadmin
Client Version	14.1.7.0

Scan Profile

Target	XCS-2K22
Profile Name	Scan Windows
Profile Identifier	f3fc8979-14a3-43e7-b931-4f06e4a3c726

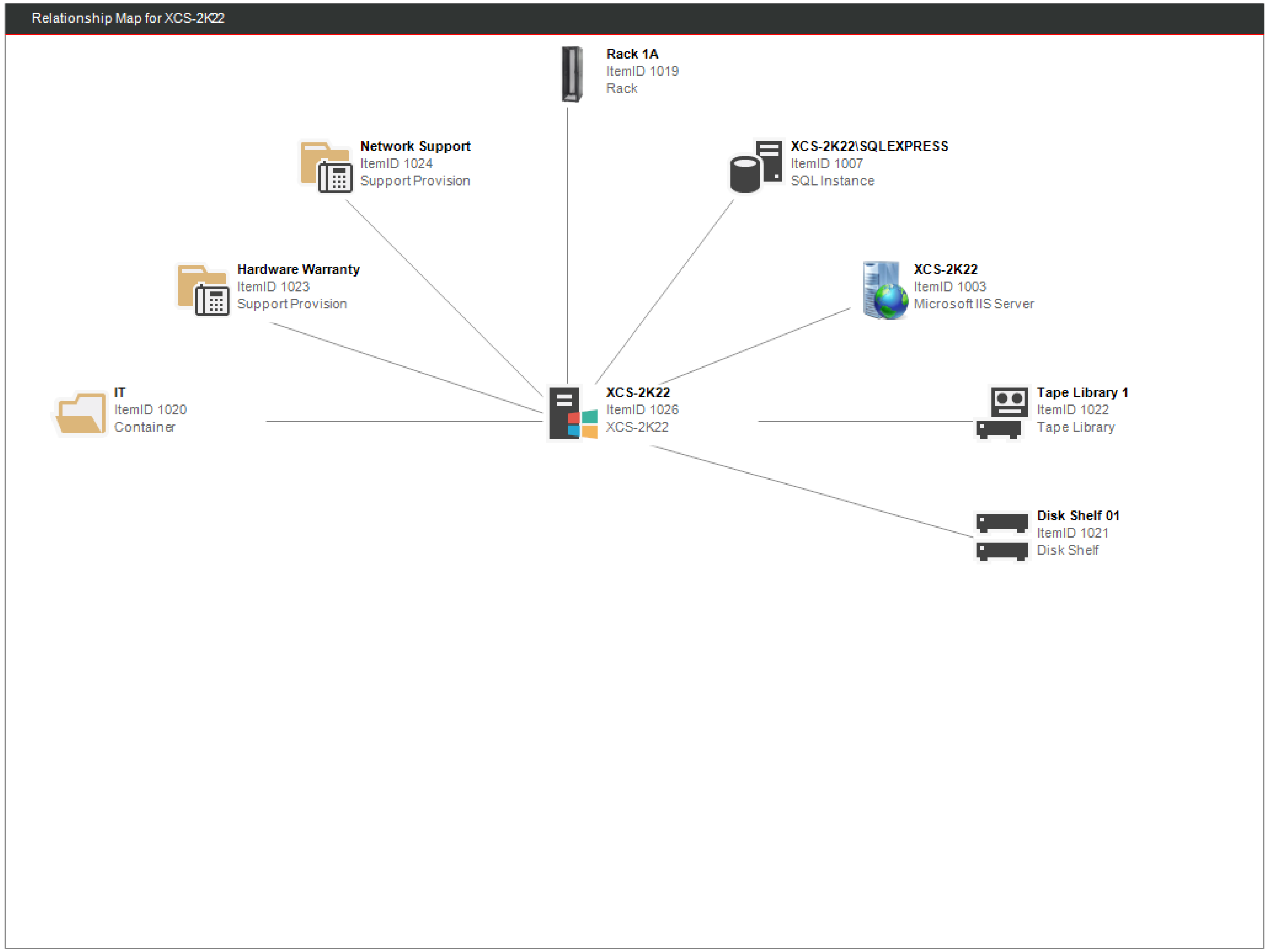
Relationships

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

8 Relationships

Item ID	Direction	Name	Type	Relationship Type
1020	Outbound	IT	Container	Contained Within
1023	Outbound	Hardware Warranty	Support Provision	Is Maintained By
1024	Outbound	Network Support	Support Provision	Is Supported By
1019	Outbound	Rack 1A	Rack	Located Within
1007	Outbound	XCS-2K22\SQLEXPRESS	SQL Instance	Hosts SQL Instance
1003	Outbound	XCS-2K22	Microsoft IIS Server	Hosts IIS Server
1022	Outbound	Tape Library 1	Tape Library	Connected Tape Library
1021	Outbound	Disk Shelf 01	Disk Shelf	Connected Disk Shelf

Relationship Map



Management Summary

Provides a management summary for this machine

Operating System

Operating System Name	Microsoft Windows Server 2022 Datacenter
Service Pack	[None Installed]

Naming and Role

Domain	test2022.net
Domain Role	Member Server
NetBIOS Name	XCS-2K22
Fully Qualified Domain Name	xcs-2k22.test2022.net

Hardware Information

Serial Number	VMware-56 4d 42 da e0 b5 8b 9e-c0 ea ef f4 59 bd 06 dd
Manufacturer	HP
Model	ProLiant DL360 G4
Asset Tag	AT-426232
Product Number	24-10526-60442

Networking

IPv4 Addresses	192.168.131.246/24
IPv6 Addresses	fe80::8032:2d0f:4e06:f641%12/0.0.0.64

Remote Desktop Settings

Allow Connections	False

Server Functions

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

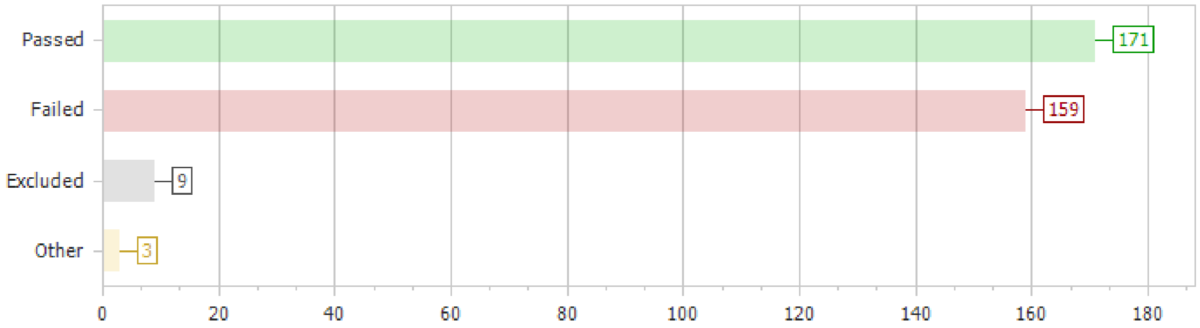
Compliance Benchmarks

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

Name	Version	Passed	Failed	Other
Windows Basic Compliance Benchmark	5.0.0.0	171	159	3

Windows Basic Compliance Benchmark [5.0.0.0]

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



342 Benchmark Results

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

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

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

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

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

✓ 13.24	Set the "Force shutdown from a remote system" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✓ 13.25	Set the "Generate security audits" user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\adfssrv NT SERVICE\drs	IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE
✓ 13.26	Set the "Impersonate a client after authentication" user right to include only BUILTIN\Administrators BUILTIN\IIS_IUSRS NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	BUILTIN\Administrators BUILTIN\IIS_IUSRS NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE
✓ 13.27	Set the "Increase a process working set" user right to include only BUILTIN\Device Owners BUILTIN\Users Window Manager\Window Manager Group	BUILTIN\Users
✓ 13.28	Set the "Increase scheduling priority" user right to include only BUILTIN\Administrators Window Manager\Window Manager Group	BUILTIN\Administrators Window Manager\Window Manager Group
✓ 13.29	Set the "Load and unload device drivers" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✓ 13.30	Set the "Lock pages in memory" user right to [Empty]	
✓ 13.31	Set the "Log on as a batch job" user right to include only BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\IIS_IUSRS BUILTIN\Performance Log Users	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\IIS_IUSRS BUILTIN\Performance Log Users
✗ 13.32	Set the "Log on as a service" user right to include only IIS APPPOOL\% NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\NETWORK SERVICE NT SERVICE\ALL SERVICES NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS NT SERVICE\SQLTELEMETRY$SQLEXPRESS TEST2022\sysadmin XCS-2K22\SQLServer2005SQLBrowserUser$XCS-2K22
✓ 13.33	Set the "Manage auditing and security log" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✓ 13.34	Set the "Modify an object label" user right to [Empty]	
✓ 13.35	Set the "Modify firmware environment values" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
● 13.36	Set the "Obtain an impersonation token for another user in the same session" user right to include only BUILTIN\Administrators	Unknown
✗ 13.37	Set the "Perform volume maintenance tasks" user right to include only BUILTIN\Administrators	BUILTIN\Administrators NT SERVICE\MSSQL$SQLEXPRESS
✓ 13.38	Set the "Profile single process" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
✓ 13.39	Set the "Profile system performance" user right to include only BUILTIN\Administrators NT SERVICE\WdiServiceHost	BUILTIN\Administrators NT SERVICE\WdiServiceHost
✓ 13.40	Set the "Remove computer from docking station" user right to [Any Value]	BUILTIN\Administrators
✓ 13.41	Set the "Replace a process level token" user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE	IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool

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

✗ 16.09	Set the Windows Firewall public profile log successful connections setting to "Yes"	No
Section 17: Security Options (General)		
✗ 17.01	Set the "App Runtime: Allow Microsoft accounts to be optional" security option to "Enabled"	Not Defined
✗ 17.02	Set the "Biometrics: Configure enhanced anti-spoofing" security option to "Enabled"	Not Defined
✗ 17.03	Set the "Cloud Content: Turn off Microsoft consumer experiences" security option to "Enabled"	Not Defined
✗ 17.04	Set the "Connect: Require pin for pairing" security option to "First Time" or "Always"	Not Defined
✗ 17.05	Set the "OneDrive: Prevent the usage of OneDrive for file storage" security option to "Enabled"	Not Defined
✗ 17.06	Set the "Regional and Language Options: Allow users to enable online speech recognition services" security option to "Disabled"	Not Defined
✗ 17.07	Set the "Windows Ink Workspace: Allow Windows Ink Workspace" security option to "Disabled" or "On, but disallow access above lock"	Not Defined
Section 18: Security Options (Accounts)		
✗ 18.01	Set the "Accounts: Block Microsoft accounts" security option to "Users can't add or log on with Microsoft accounts"	Not Defined
✓ 18.02	Set the "Accounts: Limit local account use of blank passwords to console logon only" security option to "Enabled"	Enabled
Section 19: Security Options (Audit)		
✓ 19.01	Set the "Audit Process Creation: Include command line in process creation events" security option to "Disabled" or "Not Defined"	Not Defined
✓ 19.02	Set the "Audit: Shut down system immediately if unable to log security audits" security option to "Disabled"	Disabled
Section 20: Security Options (Credential User Interface)		
✗ 20.01	Set the "Credential User Interface: Do not display the password reveal button" security option to "Enabled"	Not Defined
✗ 20.02	Set the "Credential User Interface: Enumerate administrator accounts on elevation" security option to "Disabled"	Not Defined
Section 21: Security Options (Credentials Delegation)		
✗ 21.01	Set the "Credentials Delegation: Encryption Oracle Remediation" security option to "Force Updated Clients"	Not Defined
✗ 21.02	Set the "Credentials Delegation: Remote host allows delegation of non-exportable credentials" security option to "Enabled"	Not Defined
Section 22: Security Options (Data Collection and Preview Builds)		
✓ 22.01	Set the "Data Collection and Preview Builds: Allow Diagnostics Data" security option to "Diagnostic data off (not recommended)" or "Send required diagnostic data" on Windows Server 2022, Windows 10 build 20348, Windows 11 and newer	Send required diagnostic data
22.02	Set the "Data Collection and Preview Builds: Allow Telemetry" security option to "0 - Security [Enterprise Only]" or "1 - Basic" on Windows Server 2016, Windows Server 2019, and Windows 10 prior to build 20348	
✗ 22.03	Set the "Data Collection and Preview Builds: Do not show feedback notifications" security option to "Enabled"	Not Defined
✗ 22.04	Set the "Data Collection and Preview Builds: Toggle user control over Insider builds" security option to "Disabled"	Enabled
Section 23: Security Options (Devices)		
✗ 23.01	Set the "Devices: Allowed to format and eject removable media" security option to "Administrators"	Not Defined
✓ 23.02	Set the "Devices: Prevent users from installing printer drivers" security option to "Enabled"	Enabled

Section 24: Security Options (Domain Controllers)

24.01	Set the "Domain controller: Allow server operators to schedule tasks" security option to "Disabled" on domain controllers	
24.02	Set the "Domain controller: LDAP server signing requirements" security option to "Require signing" on domain controllers	
24.03	Set the "Domain controller: Refuse machine account password changes" security option to "Disabled" on domain controllers	

Section 25: Security Options (Domain Members)

✗ 25.01	Set the "Domain member: Digitally encrypt or sign secure channel data (always)" security option to "Enabled" on domain members	Disabled
✗ 25.02	Set the "Domain member: Digitally encrypt secure channel data (when possible)" security option to "Enabled" on domain members	Disabled
✗ 25.03	Set the "Domain member: Digitally sign secure channel data (when possible)" security option to "Enabled" on domain members	Disabled
✗ 25.04	Set the "Domain member: Disable machine account password changes" security option to "Disabled" on domain members	Enabled
✗ 25.05	Set the "Domain member: Maximum machine account password age" security option to 30 days on domain members	0 days
✗ 25.06	Set the "Domain member: Require strong (Windows 2000 or later) session key" security option to "Enabled" on domain members	Disabled

Section 26: Security Options (Explorer Shell)

✗ 26.01	Set the "AutoPlay Policies: Disallow Autoplay for non-volume devices" security option to "Enabled"	Not Defined
✗ 26.02	Set the "AutoPlay Policies: Set the default behavior for AutoRun" security option to "Do not execute any autorun commands"	Not Defined
✗ 26.03	Set the "AutoPlay Policies: Turn off Autoplay" security option to "All drives"	Not Defined
✗ 26.04	Set the "File Explorer: Configure Microsoft Defender SmartScreen" security option to "Warn and prevent bypass"	Not Defined
✗ 26.05	Set the "File Explorer: Enable Microsoft Defender SmartScreen" security option to "Enabled"	Not Defined
✗ 26.06	Set the "File Explorer: Turn off Data Execution Prevention for Explorer" security option to "Disabled"	Not Defined
✓ 26.07	Set the "File Explorer: Turn off heap termination on corruption" security option to "Disabled" or "Not Defined"	Not Defined
✓ 26.08	Set the "File Explorer: Turn off shell protocol protected mode" security option to "Disabled" or "Not Defined"	Not Defined

Section 27: Security Options (Group Policy)

✗ 27.01	Set the "Group Policy: Continue experiences on this device" security option to "Disabled" on domain members	Not Defined
✗ 27.02	Set the "Group Policy: Registry policy processing: Do not apply during periodic background processing" security option to "Disabled" on domain members	Not Defined
✗ 27.03	Set the "Group Policy: Registry policy processing: Process even if the Group Policy objects have not changed" security option to "Enabled" on domain members	Not Defined
✓ 27.04	Set the "Group Policy: Turn off background refresh of Group Policy" security option to "Disabled" or "Not Defined" on domain members	Not Defined

Section 28: Security Options (Interactive Logon)

✗ 28.01	Set the "Interactive logon: Do not display last user name" security option to "Enabled"	Disabled
✓ 28.02	Set the "Interactive logon: Do not require CTRL+ALT+DEL" security option to "Disabled"	Disabled
✗ 28.03	Set the "Interactive logon: Machine account lockout threshold" security option to a value between 6 and 10.	Not Defined

✗ 28.04	Set the "Interactive logon: Machine inactivity limit" security option to 900 seconds or less	Not Defined
✗ 28.05	Set the "Interactive logon: Message text for users attempting to log on" security option to an appropriate value	
✗ 28.06	Set the "Interactive logon: Message title for users attempting to log on" security option to an appropriate value	
✗ 28.07	Set the "Interactive logon: Number of previous logons to cache (in case domain controller is not available)" security option to "0" for servers and "0" for workstations on domain members that are not domain controllers	11 logons
✓ 28.08	Set the "Interactive logon: Prompt user to change password before expiration" security option to a value between 5 and 10 days	5 days
✗ 28.09	Set the "Interactive logon: Require Domain Controller authentication to unlock workstation" security option to "Enabled" on domain members that are not domain controllers	Disabled
✗ 28.10	Set the "Interactive logon: Smart card removal behavior" security option to "Lock Workstation", "Force Logoff", or "Disconnect if a Remote Desktop Services session"	No Action

Section 29: Security Options (Internet Explorer - Deprecated)

✓ 29.01	Set the "Internet Explorer: Disable Internet Explorer as a stand alone browser" security option to "Disable browser never notify user", "Disable browser always notify user", or "Disable browser notify user once"	Disable browser never notify user
✗ 29.02	Set the "Internet Explorer: Prevent downloading of enclosures" security option to "Enabled"	Not Defined

Section 30: Security Options (Lanman Workstation)

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

Section 31: Security Options (Logon)

✗ 31.01	Set the "Logon: Block user from showing account details on sign-in" security option to "Enabled"	Not Defined
✗ 31.02	Set the "Logon: Do not display network selection UI" security option to "Enabled"	Not Defined
✗ 31.03	Set the "Logon: Do not enumerate connected users on domain-joined computers" security option to "Enabled" on domain members	Not Defined
✗ 31.04	Set the "Logon: Enumerate local users on domain-joined computers" security option to "Disabled" on domain members that are not domain controllers	Enabled
✗ 31.05	Set the "Logon: Turn off app notifications on the lock screen" security option to "Enabled"	Not Defined
✗ 31.06	Set the "Logon: Turn off picture password sign-in" security option to "Enabled" on domain members	Not Defined
✗ 31.07	Set the "Logon: Turn on convenience PIN sign-in" security option to "Disabled" on domain members	Not Defined
✓ 31.08	Set the "Windows Logon Options: Sign-in and lock last interactive user automatically after a restart" security setting to "Disabled"	Disabled

Section 32: Security Options (Microsoft Accounts)

✗ 32.01	Set the "Microsoft Accounts: Block all consumer Microsoft account user authentication" security option to "Enabled"	Not Defined

Section 33: Security Options (Microsoft Defender Antivirus)

✗ 33.01	Set the "Microsoft Defender Antivirus: Configure detection for potentially unwanted applications" security option to "Block"	Audit Mode
✓ 33.02	Set the "Microsoft Defender Antivirus: Configure local setting override for reporting to Microsoft MAPS" security option to "Disabled" or "Not Defined"	Not Defined
✗ 33.03	Set the "Microsoft Defender Antivirus: Configure Watson events" security option to "Disabled"	Not Defined
✓ 33.04	Set the "Microsoft Defender Antivirus: Join Microsoft MAPS" security option to "Disabled" or "Not Defined"	Not Defined

✗	33.05	Set the "Microsoft Defender Antivirus: Prevent users and apps from accessing dangerous websites" security option to "Block"	Audit Mode
✗	33.06	Set the "Microsoft Defender Antivirus: Scan removable drives" security option to "Enabled"	Not Defined
✓	33.07	Set the "Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus" security option to "Disabled" or "Not Defined"	Disabled
✓	33.08	Set the "Microsoft Defender Antivirus: Turn on behavior monitoring" security option to "Enabled" or "Not Defined"	Not Defined
✗	33.09	Set the "Microsoft Defender Antivirus: Turn on e-mail scanning" security option to "Enabled"	Not Defined

Section 34: Security Options (Microsoft Network Client)

✗	34.01	Set the "Microsoft network client: Digitally sign communications (always)" security option to "Enabled"	Disabled
✓	34.02	Set the "Microsoft network client: Digitally sign communications (if server agrees)" security option to "Enabled"	Enabled
✓	34.03	Set the "Microsoft network client: Send unencrypted password to connect to third-party SMB servers" security option to "Disabled"	Disabled

Section 35: Security Options (Microsoft Network Server)

✓	35.01	Set the "Microsoft network server: Amount of idle time required before suspending session" security option to "15 minutes"	15 minutes
✗	35.02	Set the "Microsoft network server: Digitally sign communications (always)" security option to "Enabled"	Disabled
✗	35.03	Set the "Microsoft network server: Digitally sign communications (if client agrees)" security option to "Enabled"	Disabled
✓	35.04	Set the "Microsoft network server: Disconnect clients when logon hours expire" security option to "Enabled"	Enabled
✗	35.05	Set the "Microsoft network server: Server SPN target name validation level" security option to "Accept if provided by client" or "Required from client"	Not Defined

Section 36: Security Options (MSS - Deprecated)

✓	36.01	Set the "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)" security option to "Disabled" or "Not Defined"	Disabled
✗	36.02	Set the "MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Not Defined
✗	36.03	Set the "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Not Defined
✗	36.04	Set the "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" security option to "Disabled"	Enabled
✗	36.05	Set the "MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds" security option to "300000 or 5 minutes (recommended)"	Not Defined
✗	36.06	Set the "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" security option to "Enabled"	Not Defined
✗	36.07	Set the "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)" security option to "Disabled"	Not Defined
✓	36.08	Set the "MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)" security option to "Enabled" or "Not Defined"	Not Defined
✗	36.09	Set the "MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)" security option to 5 seconds or less	Not Defined
✗	36.10	Set the "MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted" security option to 3	Not Defined
✗	36.11	Set the "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted" security option to 3	Not Defined

✗	36.12	Set the "MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning" security option to 90% or less	Not Defined
	Section 37: Security Options (Network)		
✗	37.01	Set the "DNS Client: Turn off multicast name resolution" security option to "Enabled"	Not Defined
✗	37.02	Set the "TCP/IP: NetBT NodeType" security option to "P-node (recommended)"	Not Defined
	Section 38: Security Options (Network Access)		
●	38.01	Set the "Network access: Allow anonymous SID/Name translation" security option to "Disabled" (must be set with Group Policy)	Unknown
✗	38.02	Set the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" security option to "Enabled"	Disabled
✓	38.03	Set the "Network access: Do not allow anonymous enumeration of SAM accounts" security option to "Enabled"	Enabled
✗	38.04	Set the "Network access: Do not allow storage of passwords and credentials for network authentication" security option to "Enabled"	Disabled
✓	38.05	Set the "Network access: Let Everyone permissions apply to anonymous users" security option to "Disabled"	Disabled
✓	38.06	Set the "Network access: Named Pipes that can be accessed anonymously" security option to only contain [Empty]	
✓	38.07	Set the "Network access: Remotely accessible registry paths and subpaths" security option to include only Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Perflib Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\SysmonLog	Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Perflib Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\SysmonLog
✓	38.08	Set the "Network access: Remotely accessible registry paths" security option to include only Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications	Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications
✓	38.09	Set the "Network access: Restrict anonymous access to Named Pipes and Shares" security option to "Enabled"	Enabled
✗	38.10	Set the "Network access: Restrict clients allowed to make remote calls to SAM" security option to "Administrators: Remote Access: Allow" on stand-alone machines and domain members that are not domain controllers	O:BAG:BAD:(A;;RC;;;BA)(A;;RC;;;WD)
✗	38.11	Set the "Network access: Shares that can be accessed anonymously" security option to an empty value	Not Defined
✓	38.12	Set the "Network access: Sharing and security model for local accounts" security option to "Classic - Local users authenticate as themselves"	Classic - local users authenticate as themselves
	Section 39: Security Options (Network Connections)		
✗	39.01	Set the "Network Connections: Prohibit installation and configuration of Network Bridge on your DNS domain network" security option to "Enabled"	Not Defined
✗	39.02	Set the "Network Connections: Prohibit use of Internet Connection Sharing on your DNS domain network" security option to "Enabled"	Not Defined

✗	39.03	Set the "Network Connections: Require domain users to elevate when setting a network's location" security option to "Enabled"	Not Defined
Section 40: Security Options (Network Provider)			
✓	40.01	Set the "Network Provider: Hardened UNC Paths" security option to *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1	
Section 41: Security Options (Network Security)			
✗	41.01	Set the "Network security: Allow Local System to use computer identity for NTLM" security option to "Enabled"	Not Defined
✗	41.02	Set the "Network security: Allow LocalSystem NULL session fallback" security option to "Disabled"	Not Defined
✗	41.03	Set the "Network security: Allow PKU2U authentication requests to this computer to use online identities" security option to "Disabled" on domain members	Enabled
✗	41.04	Set the "Network security: Configure encryption types allowed for Kerberos" security option to "AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types" on domain members	DES_CBC_CRC DES_CBC_MD5 RC4_HMAC_MD5 AES128_HMAC_SHA1 AES256_HMAC_SHA1 Future encryption types
✓	41.05	Set the "Network security: Do not store LAN Manager hash value on next password change" security option to "Enabled"	Enabled
●	41.06	Set the "Network security: Force logoff when logon hours expire" security option to "Enabled"	Unknown
✗	41.07	Set the "Network security: LAN Manager authentication level" security option to "Send NTLMv2 response only. Refuse LM & NTLM"	Not Defined
✗	41.08	Set the "Network security: LDAP client signing requirements" security option to "Require Signing"	Negotiate Signing
✗	41.09	Set the "Network security: Minimum session security for NTLM SSP based (including secure RPC) clients" security option to "Require NTLMv2 session security, Require 128-bit encryption"	Require 128-bit encryption
✗	41.10	Set the "Network security: Minimum session security for NTLM SSP based (including secure RPC) servers" security option to "Require NTLMv2 session security, Require 128-bit encryption"	Require 128-bit encryption
Section 42: Security Options (Personalization)			
✓	42.01	Set the "Personalization: Prevent enabling lock screen camera" security option to "Enabled"	Enabled
✓	42.02	Set the "Personalization: Prevent enabling lock screen slide show" security option to "Enabled"	Enabled
Section 43: Security Options (Recovery Console)			
✓	43.01	Set the "Recovery console: Allow automatic administrative logon" security option to "Disabled"	Disabled
✓	43.02	Set the "Recovery Console: Allow floppy copy and access to drives and folders" security option to "Disabled"	Disabled
Section 44: Security Options (Remote Assistance)			
✗	44.01	Set the "Remote Assistance: Allow Offer Remote Assistance" security option to "Disabled"	Not Defined
✗	44.02	Set the "Remote Assistance: Allow Solicited Remote Assistance" security option to "Disabled"	Not Defined
Section 45: Security Options (Remote Desktop Connection Client)			
✗	45.01	Set the "Remote Desktop Connection Client: Do not allow passwords to be saved" security option to "Enabled"	Not Defined
Section 46: Security Options (Remote Procedure Call)			
✓	46.01	Set the "Remote Procedure Call: Enable RPC Endpoint Mapper Client Authentication" security option to "Enabled" on domain members that are not domain	Enabled

	controllers	
✓ 46.02	Set the "Remote Procedure Call: Restrict Unauthenticated RPC clients" security option to "Authenticated" on domain members that are not domain controllers	Authenticated
Section 47: Security Options (Search)		
✗ 47.01	Set the "Search: Allow Cloud Search" security option to "Disable Cloud Search"	Not Defined
✓ 47.02	Set the "Search: Allow indexing of encrypted files" security option to "Disabled" or "Not Defined"	Not Defined
Section 48: Security Options (Security Providers)		
✓ 48.01	Set the "Security Providers: WDigest Authentication" security option to "Disabled" or "Not Defined"	Not Defined
Section 49: Security Options (Startup and Shutdown)		
✓ 49.01	Set the "Early Launch Antimalware: Boot-Start Driver Initialization Policy" security option to "Good, unknown and bad but critical" or "Not Defined"	Not Defined
✓ 49.02	Set the "Shutdown: Allow system to be shut down without having to log on" security option to "Disabled" (only applies to server operating systems)	Disabled
✗ 49.03	Set the "Shutdown: Clear virtual memory pagefile" security option to "Enabled"	Disabled
Section 50: Security Options (System Cryptography)		
✗ 50.01	Set the "System cryptography: Force strong key protection for user keys stored on the computer" security option to "User is prompted when the key is first used" or higher	Not Defined
Section 51: Security Options (System Objects)		
✓ 51.01	Set the "System objects: Require case insensitivity for non-Windows subsystems" security option to "Enabled"	Enabled
✓ 51.02	Set the "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)" security option to "Enabled"	Enabled
Section 52: Security Options (System Settings)		
✓ 52.01	Set the "System settings: Optional subsystems" security option to include only [Empty]	
✗ 52.02	Set the "System settings: Use certificate rules on Windows executables for Software Restriction Policies" security option to "Enabled"	Disabled
Section 53: Security Options (User Account Control)		
✗ 53.01	Set the "User Account Control: Admin Approval Mode for the Built-in Administrator account" security option to "Enabled"	Not Defined
✓ 53.02	Set the "User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop" security option to "Disabled"	Disabled
✗ 53.03	Set the "User Account Control: Apply UAC restrictions to local accounts on network logons" security option to "Enabled"	Not Defined
✗ 53.04	Set the "User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode" security option to "Prompt for consent on the secure desktop"	Prompt for consent for non-Windows binaries
✗ 53.05	Set the "User Account Control: Behavior of the elevation prompt for standard users" security option to "Automatically deny elevation requests"	Prompt for credentials
✓ 53.06	Set the "User Account Control: Detect application installations and prompt for elevation" security option to "Enabled"	Enabled
✓ 53.07	Set the "User Account Control: Only elevate UIAccess applications that are installed in secure locations" security option to "Enabled"	Enabled
✓ 53.08	Set the "User Account Control: Run all administrators in Admin Approval Mode" security option to "Enabled"	Enabled
✓ 53.09	Set the "User Account Control: Switch to the secure desktop when prompting for elevation" security option to "Enabled"	Enabled
✓ 53.10	Set the "User Account Control: Virtualize file and registry write failures to per-user locations" security option to "Enabled"	Enabled

Section 54: Security Options (Windows Connection Manager)

✓	54.01	Set the "Windows Connection Manager: Minimize the number of simultaneous connections to the Internet or a Windows Domain" security option to "1 = Minimize simultaneous connections" or "Not Defined"	Not Defined
✓	54.02	Set the "Windows Connection Manager: Prohibit connection to non-domain networks when connected to domain authenticated network" security option to "Enabled" on domain members	Enabled

Section 55: Security Options (Windows Installer)

✓	55.01	Set the "Windows Installer: Allow user control over installs" security option to "Disabled" or "Not Defined"	Not Defined
✓	55.02	Set the "Windows Installer: Always install with elevated privileges" security option to "Disabled" or "Not Defined"	Not Defined
✓	55.03	Set the "Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts'" security option to "Disabled" or "Not Defined"	Not Defined

Section 56: Security Options (Windows PowerShell)

✗	56.01	Set the "Windows PowerShell: Turn on PowerShell Script Block Logging" security option to "Enabled"	Not Defined
✗	56.02	Set the "Windows PowerShell: Turn on PowerShell Transcription" security option to "Enabled"	Not Defined

Section 57: Security Options (Windows Security)

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

Location

Provides details of the physical location of this Windows machine.

Contoso Technical Services DC01

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

Room

Name	Server Room 1

Rack

Name	Rack 1A

Hardware

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

Hardware Information

Serial Number	VMware-56 4d 42 da e0 b5 8b 9e-c0 ea ef f4 59 bd 06 dd
Manufacturer	HP
Model	ProLiant DL360 G4
Asset Tag	AT-426232
Product Number	24-10526-60442

ProLiant DL360 G4

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	4,071MB
UUID	DA424D56-B5E0-9E8B-C0EA-EFF459BD06DD

BIOS Information

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

VMW71.00V.18452719.B64.2108091906

Manufacturer	VMware, Inc.
Release Date	09 August 2021 01:00:00
SMBIOS BIOS Version	VMW71.00V.18452719.B64.2108091906
Version	INTEL - 6040000
Current Language	
Embedded Controller Version	255.255.0.0
Firmware Type	UEFI
System BIOS Version	255.255.0.0

CD-ROM and DVD-ROM Drives

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

1 CD-ROM and DVD-ROM Drives

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

Disk Drives

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

2 Disk Drives

Display Name	Interface	Serial Number	Partition Style	Size
[0] VMware Virtual SATA Hard Drive	Serial ATA (SATA)	00000000000000000001	Master Boot Record (MBR)	60 GB
[1] VMware Virtual NVMe Disk	NVMe	VMWare NVME_0000	GUID Partition Table (GPT)	60 GB

[0] VMware Virtual SATA Hard Drive

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

General

Model	VMware Virtual SATA Hard Drive
Firmware Revision	00000001
Bus Type	Serial ATA (SATA)
Serial Number	00000000000000000001
Size	60 GB
Location	PCI Slot 36 : Bus 2 : Device 4 : Function 0 : Adapter 2 : Port 0
Capabilities	Random Access Supports Writing SMART Notification
Partition Style	Master Boot Record (MBR)
Bytes Per Sector	512
Sectors Per Track	63

Status

Operational Status	OK

Storage Pools

Storage Pool Names	Primordial

1 Partitions

Identifier	Active	Type	Size
Disk #0, Partition #0	False	Basic (MBR)	60 GB

E:

Active	False
DeviceId	Disk #0, Partition #0
Partition Type	Basic (MBR)
File System	ReFS
Volume Name	ReFS Volume
Volume Serial Number	DC483EFD
Size	59.94 GB

E: (98% 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	1.0
Bus Type	NVMe
Serial Number	VMWare NVME_0000
Size	60 GB
Location	nvme0
GUID	{a63b8588-2640-4f03-adf6-01a5a21d30e5}
Capabilities	Random Access Supports Writing
Partition Style	GUID Partition Table (GPT)
Bytes Per Sector	512
Signature	
Sectors Per Track	63

Status

Operational Status	OK

Storage Pools

Storage Pool Names	Primordial

Unallocated Space

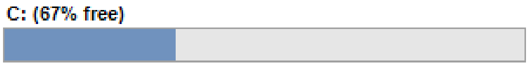
Unallocated Space	15 MB

3 Partitions

Identifier	Active	Type	Size
Disk #1, Partition #0	True	Other	100 MB
Disk #1, Partition #1	False	Basic (GPT)	59.37 GB
Disk #1, Partition #2	False	Other (GPT)	523 MB

C:

Active	False
DeviceId	Disk #1, Partition #1
Partition Type	Basic (GPT)
File System	NTFS
Volume Name	
Volume Serial Number	B693A3CA
Size	59.37 GB



Disk Shelves

Provides information about the disk shelves connected to this machine.

1 Connected Disk Shelves

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

Disk Shelf 01

Disk Shelf 01

Item ID	1021
Description	Windows servers disk shelf.
Primary Owner Name	Technical Services
Primary Owner Contact	technicalservices@contosofoods.com

Hardware Information

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

Volumes

Provides information about the volumes found on this Windows machine.

4 Volumes

Name	Total Size	Free Space	Shadow Copy
C:	59.37 GB	39.66 GB	False
E: (ReFS Volume)	59.94 GB	58.68 GB	False
EFI System Partition (a4843695-894b-4c80-b1fe-ebc21feb01fc)	96 MB	67.3 MB	False
Recovery Partition (462dd327-6aac-4b83-a6e9-7bfa44242e04)	523 MB	85.68 MB	False

C:

Provides information about the volumes found on this Windows machine.

Volume Details

Block Size	4,096
Capacity	59.37 GB
Drive Letter	C:
File System	NTFS
Label	
Volume Identifier	1a1e138d-f439-483a-a498-67110314debf
Used Space	19.71 GB
Free Space	39.66 GB

C: (67% free)

Shadow Copy Configuration

Enabled	False

Disk Quota

State	Disabled

Security

Owner	NT SERVICE\TrustedInstaller

6 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 folders / append data	This folder and subfolders
BUILTIN\Users	False	Allow	Create files / write data	Subfolders 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	This folder, subfolders and files

1 NTFS Audit Rules

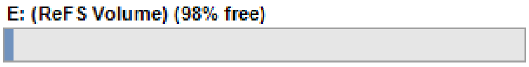
Account Name	Inherited	Type	Rights	Applies To
TEST2022\sysadmin	False	Success	Read & execute	This folder, subfolders and files

E: (ReFS Volume)

Provides information about the volumes found on this Windows machine.

Volume Details

Block Size	4,096
Capacity	59.94 GB
Drive Letter	E:
File System	ReFS
Label	ReFS Volume
Volume Identifier	09a9e0a2-0000-0000-0000-100000000000
Used Space	1.26 GB
Free Space	58.68 GB



Shadow Copy Configuration

Enabled	False

Security

Owner	BUILTIN\Administrators

6 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 folders / append data	This folder and subfolders
BUILTIN\Users	False	Allow	Create files / write data Read & execute	This folder, subfolders and files
CREATOR OWNER	False	Allow	Full control	Subfolders and files only
Everyone	False	Allow	Read & execute	This folder, subfolders and files
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 (a4843695-894b-4c80-b1fe-ebc21feb01fc)

Provides information about the volumes found on this Windows machine.

Volume Details

Block Size	1,024
Capacity	96 MB
Drive Letter	
File System	FAT32
Label	
Volume Identifier	a4843695-894b-4c80-b1fe-ebc21feb01fc
Used Space	28.7 MB
Free Space	67.3 MB

Shadow Copy Configuration

Enabled	False

Recovery Partition (462dd327-6aac-4b83-a6e9-7bfa44242e04)

Provides information about the volumes found on this Windows machine.

Volume Details

Block Size	4,096
Capacity	523 MB
Drive Letter	
File System	NTFS
Label	
Volume Identifier	462dd327-6aac-4b83-a6e9-7bfa44242e04
Used Space	437.32 MB
Free Space	85.68 MB

Drive (16% free)

Shadow Copy Configuration

Enabled	False

Devices

Provides details about the devices and drivers on this machine.

Batteries

Name	Driver Provider	Driver Version	Status
Microsoft AC Adapter	Microsoft	10.0.20348.1	Device is working properly.

Computer

Name	Driver Provider	Driver Version	Status
ACPI x64-based PC	Microsoft	10.0.20348.1	Device is working properly.

Disk drives

Name	Driver Provider	Driver Version	Status
VMware Virtual NVMe Disk	Microsoft	10.0.20348.1	Device is working properly.
VMware Virtual SATA Hard Drive	Microsoft	10.0.20348.1	Device is working properly.

Display adapters

Name	Driver Provider	Driver Version	Status
VMware SVGA 3D	VMware, Inc.	8.17.3.5	Device is working properly.

DVD/CD-ROM drives

Name	Driver Provider	Driver Version	Status
NECVMWar VMware SATA CD01	Microsoft	10.0.20348.1	Device is working properly.

Human Interface Devices

Name	Driver Provider	Driver Version	Status
USB Input Device	Microsoft	10.0.20348.1	Device is working properly.
USB Input Device	Microsoft	10.0.20348.1	Device is working properly.

IDE ATA/ATAPI controllers

Name	Driver Provider	Driver Version	Status
ATA Channel 0	Microsoft	10.0.20348.1	Device is working properly.
ATA Channel 1	Microsoft	10.0.20348.1	Device is working properly.
Intel(R) 82371AB/EB PCI Bus Master IDE Controller	Microsoft	10.0.20348.1	Device is working properly.
Standard SATA AHCI Controller	Microsoft	10.0.20348.1	Device is working properly.

Keyboards

Name	Driver Provider	Driver Version	Status
Standard PS/2 Keyboard	Microsoft	10.0.20348.1	Device is working properly.

Mice and other pointing devices

Name	Driver Provider	Driver Version	Status
VMware Pointing Device	VMware, Inc.	12.5.10.0	Device is working properly.
VMware USB Pointing Device	VMware, Inc.	12.5.10.0	Device is working properly.
VMware USB Pointing Device	VMware, Inc.	12.5.10.0	Device is working properly.

Monitors

Name	Driver Provider	Driver Version	Status
Generic Non-PnP Monitor	Microsoft	10.0.20348.1	Device is working properly.

Network adapters

Name	Driver Provider	Driver Version	Status
Intel(R) 82574L Gigabit Network Connection	Microsoft	12.18.9.23	Device is working properly.
Microsoft Kernel Debug Network Adapter	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (GRE)	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (IKEv2)	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (IP)	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (IPv6)	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (L2TP)	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (Network Monitor)	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (PPPOE)	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (PPTP)	Microsoft	10.0.20348.1	Device is working properly.
WAN Miniport (SSTP)	Microsoft	10.0.20348.1	Device is working properly.

Ports (COM & LPT)

Name	Driver Provider	Driver Version	Status
Communications Port (COM1)	Microsoft	10.0.20348.1	Device is working properly.

Print queues

Name	Driver Provider	Driver Version	Status
Microsoft Print to PDF	Microsoft	10.0.20348.1	Device is working properly.
Microsoft XPS Document Writer	Microsoft	10.0.20348.1	Device is working properly.
Root Print Queue	Microsoft	10.0.20348.1	Device is working properly.

Processors

Name	Driver Provider	Driver Version	Status
Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	Microsoft	10.0.20348.1	Device is working properly.
Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	Microsoft	10.0.20348.1	Device is working properly.

Software devices

Name	Driver Provider	Driver Version	Status
Microsoft Radio Device Enumeration Bus	Microsoft	10.0.20348.1	Device is working properly.
Microsoft RRAS Root Enumerator	Microsoft	10.0.20348.1	Device is working properly.

Sound, video and game controllers

Name	Driver Provider	Driver Version	Status
High Definition Audio Device	Microsoft	10.0.20348.1	Device is working properly.

Storage controllers

Name	Driver Provider	Driver Version	Status
Microsoft Storage Spaces Controller	Microsoft	10.0.20348.202	Device is working properly.
Standard NVM Express Controller	Microsoft	10.0.20348.202	Device is working properly.

Storage volumes

Name	Driver Provider	Driver Version	Status
Volume	Microsoft	10.0.20348.1	Device is working properly.
Volume	Microsoft	10.0.20348.1	Device is working properly.
Volume	Microsoft	10.0.20348.1	Device is working properly.
Volume	Microsoft	10.0.20348.1	Device is working properly.
Volume	Microsoft	10.0.20348.1	Device is working properly.

Universal Serial Bus controllers

Name	Driver Provider	Driver Version	Status
Standard Enhanced PCI to USB Host Controller	Microsoft	10.0.20348.1	Device is working properly.
Standard Universal PCI to USB Host Controller	Microsoft	10.0.20348.1	Device is working properly.
Standard USB 3.1 eXtensible Host Controller - 1.0 (Microsoft)	Microsoft	10.0.20348.1	Device is working properly.
USB Composite Device	Microsoft	10.0.20348.1	Device is working properly.
USB Root Hub	Microsoft	10.0.20348.1	Device is working properly.
USB Root Hub	Microsoft	10.0.20348.1	Device is working properly.
USB Root Hub (USB 3.0)	Microsoft	10.0.20348.1	Device is working properly.

Physical Memory

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

Physical Memory

Total Physical Memory	4,071MB

8 Physical Memory Devices

Location	Manufacturer	Serial Number	Capacity	Part Number	Speed
RAM slot #0	VMware Virtual RAM	00000001	2,048MB	VMW-2048MB	Unknown
RAM slot #1	VMware Virtual RAM	00000002	1,024MB	VMW-1024MB	Unknown
RAM slot #2	VMware Virtual RAM	00000003	512MB	VMW-512MB	Unknown
RAM slot #3	VMware Virtual RAM	00000004	256MB	VMW-256MB	Unknown
RAM slot #4	VMware Virtual RAM	00000005	128MB	VMW-128MB	Unknown
RAM slot #5	VMware Virtual RAM	00000006	64MB	VMW-64MB	Unknown
RAM slot #6	VMware Virtual RAM	00000007	32MB	VMW-32MB	Unknown
RAM slot #7	VMware Virtual RAM	00000008	8MB	VMW-8MB	Unknown

Printers

Provides details of the printers connected to the Windows machine.

🖶 2 Printers

Name	Location	Comment	Share Name
🖶 Microsoft XPS Document Writer			[Not Shared]
🖶 Microsoft Print to PDF			[Not Shared]

Microsoft XPS Document Writer

Provides details of the printers connected to the Windows machine.

Printer Properties

Comment	
Capabilities	Copies Color Collate
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 XPS Document Writer v4

Share Configuration

Share Name	[Not Shared]

Permissions

Type	Principal	Access
Allow	XCS-2K22\Administrator	Manage Documents, Manage Printer, Print
Allow	CREATOR OWNER	Manage Documents
Allow	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Manage Documents, Print
Allow	Everyone	Print
Allow	BUILTIN\Administrators	Manage Documents, Manage Printer, Print
? Allow	S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-1087000422	Manage Documents, Print

Microsoft Print to PDF

Provides details of the printers connected to the Windows machine.

Printer Properties

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

Advanced

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

Share Configuration

Share Name	[Not Shared]

Permissions

Type	Principal	Access
Allow	XCS-2K22\Administrator	Manage Documents, Manage Printer, Print
Allow	CREATOR OWNER	Manage Documents
Allow	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Manage Documents, Print
Allow	Everyone	Print
Allow	BUILTIN\Administrators	Manage Documents, Manage Printer, Print
? Allow	S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-1087000422	Manage Documents, Print

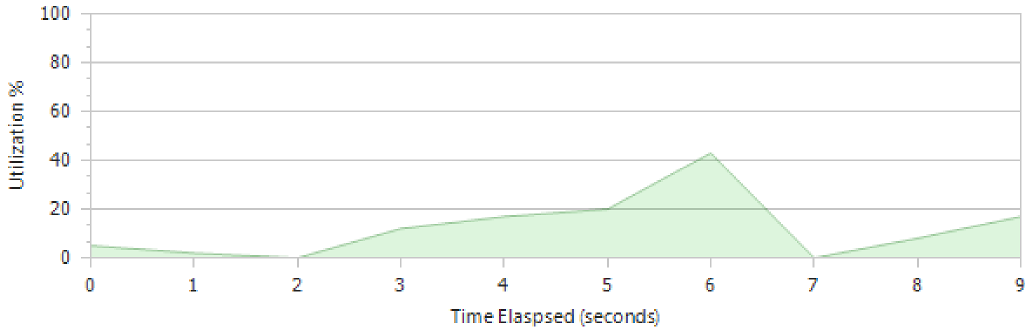
Processors

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

2 Processors

Device ID	Name	Status	Cores
CPU0	Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	Enabled	1
CPU1	Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	Enabled	1

Total Processor Utilization



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

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

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

CPU Status	Enabled
Current Clock Speed	2,400MHz
Description	Intel64 Family 6 Model 165 Stepping 2
Device Identifier	CPU0
Manufacturer	GenuineIntel
Number Of Cores	1
NumberOfLogicalProcessors	1
Processor Id	0F8BFBFF000A0652
Socket Designation	CPU 0

Virtualization Settings

Address Translation Extensions	False
Virtualization Firmware Enabled	False

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

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

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

CPU Status	Enabled
Current Clock Speed	2,400MHz
Description	Intel64 Family 6 Model 165 Stepping 2
Device Identifier	CPU1
Manufacturer	GenuineIntel
Number Of Cores	1
NumberOfLogicalProcessors	1
Processor Id	0F8BFBFF000A0652
Socket Designation	CPU 1

Virtualization Settings

Address Translation Extensions	False
Virtualization Firmware Enabled	False

Tape Libraries

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

1 Connected Tape Libraries

Name	Manufacturer	Model	Product Number
Tape Library 1	Contoso Hardware	MTL01	PN009

Tape Library 1

Tape Library 1

Item ID	1022
Description	Windows servers tape library.
Primary Owner Name	Technical Services
Primary Owner Contact	technicalservices@contosofoods.com

Hardware Information

Serial Number	SN03
Manufacturer	Contoso Hardware
Model	MTL01
Asset Tag	AT7212
Product Number	PN009

Video Controllers

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

1 Video Controllers

Name	Adapter Memory	Driver Version
VMware SVGA 3D	256 MB	8.17.3.5

VMware SVGA 3D

DAC Type	n/a
Adapter RAM	256 MB
Driver Date	06 July 2021 01:00:00
Driver Version	8.17.3.5
Inf Filename	oem8.inf
Drivers	vm3dum64_loader.dll
Maximum Refresh Rate	64Hz
Video Mode Description	3143 x 1991 x 4294967296 colors

Networking

Provides networking information for the Windows machine.

Networking Information

Network Adapters	14 Network Adapters
IPv4 Addresses	192.168.131.246/24
IPv6 Addresses	fe80::8032:2d0f:4e06:f641%12/0.0.0.64

Advanced

SNMP Installed	False
Routing Table Entries	11
Shares	5

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	08 May 2021 09:20:29
Last Accessed	08 May 2021 09:18:32
Last Modified	08 May 2021 09:18:32
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
? APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES	True	Allow	Read & execute	This folder or file only
BUILTIN\Administrators	True	Allow	Full control	This folder or file only
BUILTIN\Users	True	Allow	Read & execute	This folder or file only
NT AUTHORITY\SYSTEM	True	Allow	Full control	This folder or file only

0 NTFS Audit Rules

There are no audit rules found.

File Contents

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
```

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

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

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-BD-06-DD

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	0012
Device Name	Intel(R) 82574L Gigabit Network Connection
MAC Address	00-0C-29-BD-06-DD
Status	Device is working properly.
Driver Date	2020-06-10
Driver Version	12.18.9.23
Physical Adapter	True
Interface GUID	{BB6B4EE3-2DEF-4784-B7A7-0C4139B2A0BE}
Speed / Duplex	1 Gbps [Full Duplex]

Network Adapter Bindings

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

Network Category

Name	Domain network

IP Configuration

DHCP Enabled	True
IP Addresses	fe80::8032:2d0f:4e06:f641%12/0.0.0.64 192.168.131.246/24
Default Gateways	192.168.131.2
DHCP Server	192.168.131.254

DNS Settings

DNS Hostname	XCS-2K22
DNS Domain	localdomain
DNS Suffixes	test2022.net localdomain
DNS Servers	192.168.131.221
Register in DNS	True
Use Connection's Suffix in DNS Registration	False

WINS Settings

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

Advanced Properties

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

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

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

IPv4 Routing Table

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

11 Active Routes

Destination	Subnet Mask	Gateway	Interface	Metric	Protocol
255.255.255.255	255.255.255.255	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
255.255.255.255	255.255.255.255	0.0.0.0		331	Local
224.0.0.0	240.0.0.0	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
224.0.0.0	240.0.0.0	0.0.0.0		331	Local
192.168.131.255	255.255.255.255	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
192.168.131.246	255.255.255.255	0.0.0.0	Intel(R) 82574L Gigabit Network Connection	281	Local
192.168.131.0	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	192.168.131.2	Intel(R) 82574L Gigabit Network Connection	25	NetMgmt

Remote Assistance

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

❓ Remote Assistance Settings

Enabled	False

Remote Desktop

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

Remote Desktop Settings

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

SNMP Configuration

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

SNMP Settings

Installed	False

Shares

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

5 Shares

Name	Path	Type	Description
ADMIN$	C:\Windows	Administrative Share	Remote Admin
C$	C:\	Administrative Share	Default share
E$	E:\	Administrative Share	Default share
IPC$		Administrative IPC Queue	Remote IPC
Shared Folder	C:\Shared Folder	File Share	This is a Windows 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
? APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES	False	Allow	Read & execute	This folder, subfolders and files
BUILTIN\Administrators	False	Allow	Full control	Subfolders and files only
BUILTIN\Administrators	False	Allow	Modify	This folder or file only
BUILTIN\Users	False	Allow	Read & execute	This folder, subfolders and files
CREATOR OWNER	False	Allow	Full control	Subfolders and files only
NT AUTHORITY\SYSTEM	False	Allow	Full control	Subfolders and files only
NT AUTHORITY\SYSTEM	False	Allow	Modify	This folder or file only
NT SERVICE\TrustedInstaller	False	Allow	Full control	This folder and subfolders

0 NTFS Audit Rules

There are no audit rules found.

C$

C$

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

Security

Owner	NT SERVICE\TrustedInstaller

6 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 folders / append data	This folder and subfolders
BUILTIN\Users	False	Allow	Create files / write data	Subfolders 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	This folder, subfolders and files

1 NTFS Audit Rules

Account Name	Inherited	Type	Rights	Applies To
TEST2022\sysadmin	False	Success	Read & execute	This folder, subfolders and files

E$

E$

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

Security

Owner	BUILTIN\Administrators

6 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 folders / append data	This folder and subfolders
BUILTIN\Users	False	Allow	Create files / write data Read & execute	This folder, subfolders and files
CREATOR OWNER	False	Allow	Full control	Subfolders and files only
Everyone	False	Allow	Read & execute	This folder, subfolders and files
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

Shared Folder

Shared Folder

Description	This is a Windows share.
Allow Maximum	True
Path	C:\Shared Folder
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

Share Permissions

Account Name	Action	Rights
Everyone	Allow	Read

Security

Owner	TEST2022\sysadmin

6 NTFS Permissions

Account Name	Inherited	Action	Rights	Applies To
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 files / write data Create folders / append data	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
TEST2022\sysadmin	True	Allow	Full control	This folder or file only

0 NTFS Audit Rules

There are no audit rules found.

Security

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

Security Identifiers

Machine SID	S-1-5-21-1216405789-3367079517-4022053389
Computer Domain SID	S-1-5-21-509945820-3428461454-1774803006-1105

Local Administrator

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

Guest Account

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

Local Administrators

Name	Administrators
Description	Administrators have complete and unrestricted access to the computer/domain
Members	S-1-5-32-579 XCS-2K22\Administrator

Advanced Audit Policy

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

Account Logon

Subcategory	Audit Events	Configuration Source
Audit Credential Validation	Success	Default Domain Policy
Audit Kerberos Authentication Service		Local
Audit Kerberos Service Ticket Operations		Local
Audit Other Account Logon Events		Local

Account Management

Subcategory	Audit Events	Configuration Source
Audit Application Group Management		Local
Audit Computer Account Management		Local
Audit Distribution Group Management		Local
Audit Other Account Management Events		Local
Audit Security Group Management		Local
Audit User Account Management		Local

Detailed Tracking

Subcategory	Audit Events	Configuration Source
Audit DPAPI Activity		Local
Audit PNP Activity		Local
Audit Process Creation		Local
Audit Process Termination		Local
Audit RPC Events		Local

DS Access

Subcategory	Audit Events	Configuration Source
Audit Detailed Directory Service Replication		Local
Audit Directory Service Access		Default Domain Policy
Audit Directory Service Changes		Default Domain Policy
Audit Directory Service Replication	Failure	Default Domain Policy

Logon/Logoff

Subcategory	Audit Events	Configuration Source
Audit Account Lockout		Local
Audit Group Membership		Local
Audit IPsec Extended Mode		Local
Audit IPsec Main Mode		Local
Audit IPsec Quick Mode		Local
Audit Logoff		Local
Audit Logon		Local
Audit Network Policy Server		Local
Audit Other Logon/Logoff Events		Local
Audit Special Logon		Local
Audit User / Device Claims		Local

Object Access

Subcategory	Audit Events	Configuration Source
Audit Application Generated		Local
Audit Central Access Policy Staging		Local
Audit Certification Services		Local
Audit Detailed File Share		Local
Audit File Share		Local
Audit File System		Local
Audit Filtering Platform Connection		Local
Audit Filtering Platform Packet Drop		Local
Audit Handle Manipulation		Local
Audit Kernel Object		Local
Audit Other Object Access Events		Local
Audit Registry		Local
Audit Removable Storage		Local
Audit SAM		Local

Policy Change

Subcategory	Audit Events	Configuration Source
Audit Audit Policy Change		Local
Audit Authentication Policy Change		Local
Audit Authorization Policy Change		Local
Audit Filtering Platform Policy Change		Local
Audit MPSSVC Rule-Level Policy Change		Local
Audit Other Policy Change Events		Local

Privilege Use

Subcategory	Audit Events	Configuration Source
Audit Non Sensitive Privilege Use		Local
Audit Other Privilege Use Events		Local
Audit Sensitive Privilege Use		Local

System

Subcategory	Audit Events	Configuration Source
Audit IPsec Driver		Local
Audit Other System Events		Local
Audit Security State Change		Local
Audit Security System Extension		Local
Audit System Integrity		Local

Audit Policy

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

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

Certificate Stores

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

Store Name	Certificate Count
Intermediate Certification Authorities	3
Personal	1
Third-Party Root Certification Authorities	16
Trusted People	0
Trusted Publisher	0
Trusted Root Certification Authorities	13
Web Hosting	0

Personal

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

1 Certificates

Subject	Issuer	Expiry Date
WMSvc-SHA2-XCS-2K22	WMSvc-SHA2-XCS-2K22	30 August 2031

WMSvc-SHA2-XCS-2K22

Provides details of the X.509 certificate.

General

Subject Name	WMSvc-SHA2-XCS-2K22
Subject	CN=WMSvc-SHA2-XCS-2K22
Issuer	CN=WMSvc-SHA2-XCS-2K22
Issuer Name	WMSvc-SHA2-XCS-2K22
Valid From	01 September 2021
Expiry Date	30 August 2031
Key Usage	Data encipherment Digital Signature Key encipherment
Enhanced Key Usages	Server Authentication (1.3.6.1.5.5.7.3.1)

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	2D33ED46053885814A11C3ED13F38CAA
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	WMSVC-SHA2
Thumbprint	FBC432C75BC858C9F3788080D1F0C25423DC20DC
Purposes	Enable all purposes for this certificate

Web Hosting

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

> There are no certificates in this store.

Local Account Policies

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

Account Lockout Policy

Policy	Policy Setting	Configuration Source
Account Lockout Duration	Not Applicable	Configured Locally
Account Lockout Threshold	0 invalid login attempt(s)	Configured Locally
Reset Account Lockout 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
Store passwords using reversible encryption	False	Default Domain Policy

LAPS Settings

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

General Settings

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

Policy Settings

Administrator Account Name	test2022\sysadmin
Password Age (Days)	30
Password Length	14
Password Complexity Type	Large Letters + Small Letters + Numbers + Specials

Local Users

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

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

Administrator

Provides details of this local account.

Account Details

Name	Administrator
Description	Built-in account for administering the computer/domain
Enabled	True
Password Never Expires	True
Full Name	Administrator Account
Security Identifier	S-1-5-21-1216405789-3367079517-4022053389-500
Last Login	02/08/2022 14:08:04
Password Expired	False
Password Last Set	31 August 2022 16:59:46
User Cannot Change Password	False

Profile

Profile Path	\\DC-2K22\Profiles\Administrator
Login Script	Administrator.ps1
Home Drive	Z:
Home Directory	\\DC-2K22\Home\Administrator

DefaultAccount

Provides details of this local account.

Account Details

Name	DefaultAccount
Description	A user account managed by the system.
Enabled	False
Password Never Expires	True
Full Name	
Security Identifier	S-1-5-21-1216405789-3367079517-4022053389-503
Last Login	Never
Password Expired	False
Password Last Set	Never
User Cannot Change Password	False

Profile

Profile Path	
Login Script	
Home Drive	
Home Directory	

Guest

Provides details of this local account.

Account Details

Name	Guest
Description	Built-in account for guest access to the computer/domain
Enabled	False
Password Never Expires	True
Full Name	
Security Identifier	S-1-5-21-1216405789-3367079517-4022053389-501
Last Login	Never
Password Expired	False
Password Last Set	Never
User Cannot Change Password	True

Profile

Profile Path	
Login Script	
Home Drive	
Home Directory	

WDAGUtilityAccount

Provides details of this local account.

Account Details

Name	WDAGUtilityAccount
Description	A user account managed and used by the system for Windows Defender Application Guard scenarios.
Enabled	False
Password Never Expires	False
Full Name	
Security Identifier	S-1-5-21-1216405789-3367079517-4022053389-504
Last Login	Never
Password Expired	True
Password Last Set	[Password Expired]
User Cannot Change Password	False

Profile

Profile Path	
Login Script	
Home Drive	
Home Directory	

Local Groups

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

Access Control Assistance Operators

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

Administrators

Description	Administrators have complete and unrestricted access to the computer/domain
Security Identifier	S-1-5-32-544
Members	S-1-5-32-579 XCS-2K22\Administrator

Backup Operators

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

Certificate Service DCOM Access

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

Cryptographic Operators

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

Device Owners

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

Distributed COM Users

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

Event Log Readers

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

Guests

Description	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Security Identifier	S-1-5-32-546
Members	XCS-2K22\Guest

Hyper-V Administrators

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

IIS_IUSRS

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

Network Configuration Operators

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

Performance Log Users

Description	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer
Security Identifier	S-1-5-32-559
Members	

Performance Monitor Users

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

Power Users

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

Print Operators

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

RDS Endpoint Servers

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

RDS Management Servers

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

RDS Remote Access Servers

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

Remote Desktop Users

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

Remote Management Users

Description	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.
Security Identifier	S-1-5-32-580
Members	

Replicator

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

SQLServer2005SQLBrowserUser$XCS-2K22

Description	Members in the group have the required access and privileges to be assigned as the log on account for the associated instance of SQL Server Browser.
Security Identifier	S-1-5-21-1216405789-3367079517-4022053389-1000
Members	NT SERVICE\SQLBrowser

Storage Replica Administrators

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

System Managed Accounts Group

Description	Members of this group are managed by the system.
Security Identifier	S-1-5-32-581
Members	XCS-2K22\DefaultAccount

Users

Description	Users are prevented from making accidental or intentional system-wide changes and can run most applications
Security Identifier	S-1-5-32-545
Members	NT AUTHORITY\Authenticated Users NT AUTHORITY\INTERACTIVE S-1-5-32-581

Microsoft Defender

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

General Settings

Product Version	4.18.2205.7
Engine Version	1.1.19500.2
Real Time Protection Enabled	True
Tamper Protection	False

Antivirus Signature

Antivirus Signature Last Updated	31 August 2022 12:32:13
Antivirus Signature Version	1.373.1302.0

Cloud

Cloud Delivered Protection Enabled	True
Automatic Cloud Sample Submission	True

Exclusions

Excluded Extensions	txt
Excluded Paths	C:\excluded file.txt C:\Excluded Folder
Excluded Processes	Task Manager

Security Options

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

232 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	Send required diagnostic data	Default Domain Policy
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	Enabled	Default Domain Policy
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	Disabled	Default Domain Policy
Domain controller: LDAP server signing requirements	None	Default Domain Policy
Domain controller: Refuse machine account password changes	Disabled	Default Domain Policy
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled	Default Domain Policy
Domain member: Digitally encrypt secure channel data (when possible)	Disabled	Default Domain Policy
Domain member: Digitally sign secure channel data (when possible)	Disabled	Default Domain Policy
Domain member: Disable machine account password changes	Enabled	Default Domain Policy
Domain member: Maximum machine account password age	0 days	Default Domain Policy
Domain member: Require strong (Windows 2000 or later) session key	Disabled	Default Domain Policy
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 display last user name	Disabled	Configured Locally
Interactive logon: Do not require CTRL+ALT+DEL	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)	11 logons	Default Domain Policy
Interactive logon: Prompt user to change password before expiration	5 days	Configured Locally

Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	Default Domain Policy
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	Disable browser never notify user	Default Domain Policy
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	Enabled	Default Domain Policy
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	Audit Mode	Default Domain Policy
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	Audit Mode	Default Domain Policy
Microsoft Defender Antivirus: Scan removable drives	Not Defined	Not Defined
Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus	Disabled	Local Group Policy
Microsoft Defender Antivirus: Turn on behavior monitoring	Not Defined	Not Defined
Microsoft Defender Antivirus: Turn on e-mail scanning	Not Defined	Not Defined
Microsoft network client: Digitally sign communications (always)	Disabled	Configured Locally
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)	Disabled	Configured Locally
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	Configured Locally
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Configured Locally
Microsoft network server: Enable SMB version 1 protocol	Not Defined	Not Defined
Microsoft network server: Enable SMB version 2 protocol	Not Defined	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined	Not Defined

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

	Server\DefaultUserConfiguration System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\SysmonLog	
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Configured Locally
Network access: Restrict clients allowed to make remote calls to SAM	O:BAG:BAD:(A;;RC;;;BA)(A;;RC;;;WD)	Default Domain Policy
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.	Enabled	Default Domain Policy
Network security: Configure encryption types allowed for Kerberos	DES_CBC_CRC DES_CBC_MD5 RC4_HMAC_MD5 AES128_HMAC_SHA1 AES256_HMAC_SHA1 Future encryption types	Default Domain Policy
Network security: Do not store LAN Manager hash value on next password change	Enabled	Configured Locally
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	Enabled	Default Domain Policy
Personalization: Prevent enabling lock screen slide show	Enabled	Default Domain Policy
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	Enabled	Default Domain Policy
Remote Procedure Call: Restrict Unauthenticated RPC clients	Authenticated	Default Domain Policy
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	Enabled	Default Domain Policy
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	365 days	Default Domain Policy
Windows Update: Defer quality updates	0 days	Default Domain Policy
Windows Update: Manage preview builds	Not Defined	Not Defined
Windows Update: Manage preview builds (Branch Readiness Level)	Not Defined	Not Defined

User Rights Assignment

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

44 User Rights

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

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

Impersonate a client after authentication	SeImpersonatePrivilege	Configured Locally	BUILTIN\Administrators BUILTIN\IIS_IUSRS NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE
Increase a process working set	SeIncreaseWorkingSetPrivilege	Configured Locally	BUILTIN\Users
Increase scheduling priority	SeIncreaseBasePriorityPrivilege	Configured Locally	BUILTIN\Administrators Window Manager\Window Manager Group
Load and unload device drivers	SeLoadDriverPrivilege	Configured Locally	BUILTIN\Administrators
Lock pages in memory	SeLockMemoryPrivilege	Configured Locally	
Log on as a batch job	SeBatchLogonRight	Configured Locally	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\IIS_IUSRS BUILTIN\Performance Log Users
Log on as a service	SeServiceLogonRight	Configured Locally	IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\DefaultAppPool NT AUTHORITY\NETWORK SERVICE NT SERVICE\ALL SERVICES NT SERVICE\MSSQL$SQLEXPRESS NT SERVICE\SQLAgent$SQLEXPRESS NT SERVICE\SQLTELEMETRY$SQLEXPRESS TEST2022\sysadmin XCS-2K22\SQLServer2005SQLBrowserUser$XCS-2K22
Manage auditing and security log	SeSecurityPrivilege	Configured Locally	BUILTIN\Administrators
Modify an object label	SeRelabelPrivilege	Configured Locally	
Modify firmware environment values	SeSystemEnvironmentPrivilege	Configured Locally	BUILTIN\Administrators
Perform volume maintenance tasks	SeManageVolumePrivilege	Configured Locally	BUILTIN\Administrators NT SERVICE\MSSQL$SQLEXPRESS
Profile single process	SeProfileSingleProcessPrivilege	Configured Locally	BUILTIN\Administrators
Profile system performance	SeSystemProfilePrivilege	Configured Locally	BUILTIN\Administrators NT SERVICE\WdiServiceHost
Remove computer from docking station	SeUndockPrivilege	Configured Locally	BUILTIN\Administrators
Replace a process-level token	SeAssignPrimaryTokenPrivilege	Configured	IIS APPPOOL\.NET v4.5

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

Windows Firewall

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

General Settings

Active Profile	Domain

Firewall Profiles

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

Domain Profile

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

Firewall State

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

Network Interfaces

Excluded Interfaces	

Settings

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

Logging Settings

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

Private Profile

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

Firewall State

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

Network Interfaces

Excluded Interfaces	

Settings

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

Logging Settings

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

Public Profile

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

Firewall State

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

Network Interfaces

Excluded Interfaces	

Settings

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

Logging Settings

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

Inbound Rules

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

87 Windows Firewall Rules

Rule Name	Profile Names	Protocol	Local Addresses	Local Ports	Remote Addresses	Remote Ports
✓ ** Dynamic TCP incoming	Any	TCP	Any	RPC	Any	Any
✓ ** TCP Port 1433	Any	TCP	Any	1433	Any	Any
✓ ** UDP Port 1434	Any	UDP	Any	1434	Any	Any
✓ AllJoyn Router (TCP-In)	Domain, Private	TCP	Any	9955	Any	Any
✓ AllJoyn Router (UDP-In)	Domain, Private	UDP	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)	Domain	TCP	Any	10246	Any	Any
✓ Cast to Device streaming server (HTTP-Streaming-In)	Public	TCP	Any	10246	PlayToDevice	Any
✓ Cast to Device streaming server (HTTP-Streaming-In)	Private	TCP	Any	10246	LocalSubnet	Any
✓ Cast to Device streaming server (RTCP-Streaming-In)	Private	UDP	Any	Any	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 (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 streaming server (RTSP-Streaming-In)	Public	TCP	Any	23554, 23555, 23556	PlayToDevice	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 - Neighbour Discovery Advertisement (ICMPv6-In)	Any	ICMPv6	Any	RPC	Any	Any
✓ Core Networking - Neighbour 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
✓ Desktop App Web Viewer	Domain, Private, Public	Any	Any	Any	Any	Any
✓ DIAL protocol server (HTTP-In)	Private	TCP	Any	10247	LocalSubnet	Any
✓ DIAL protocol server (HTTP-In)	Domain	TCP	Any	10247	Any	Any
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	Domain	ICMPv4	Any	RPC	Any	Any
✓ File and Printer Sharing (Echo Request - ICMPv6-In)	Domain	ICMPv6	Any	RPC	Any	Any
✓ File and Printer Sharing (LLMNR-UDP-In)	Domain	UDP	Any	5355	LocalSubnet	Any
✓ File and Printer Sharing (NB-Datagram-In)	Domain	UDP	Any	138	Any	Any

✓ File and Printer Sharing (NB-Name-In)	Domain	UDP	Any	137	Any	Any
✓ File and Printer Sharing (NB-Session-In)	Any	TCP	Any	139	Any	Any
✓ File and Printer Sharing (SMB-In)	Any	TCP	Any	445	Any	Any
✓ File and Printer Sharing (Spooler Service - RPC)	Domain	TCP	Any	RPC	Any	Any
✓ File and Printer Sharing (Spooler Service - RPC-EPMAP)	Domain	TCP	Any	RPCEPMap	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
✓ mDNS (UDP-In)	Domain	UDP	Any	5353	Any	Any
✓ mDNS (UDP-In)	Private	UDP	Any	5353	LocalSubnet	Any
✓ mDNS (UDP-In)	Public	UDP	Any	5353	LocalSubnet	Any
✓ Microsoft Edge (mDNS-In)	Any	UDP	Any	5353	Any	Any
✓ Microsoft Media Foundation Network Source IN [TCP 554]	Any	TCP	Any	554, 8554-8558	LocalSubnet	Any
✓ Microsoft Media Foundation Network Source IN [UDP 5004-5009]	Any	UDP	Any	5000-5020	LocalSubnet	Any
✓ Network Discovery (LLMNR-UDP-In)	Private	UDP	Any	5355	LocalSubnet	Any
✓ Network Discovery (NB-Datagram-In)	Private	UDP	Any	138	Any	Any
✓ Network Discovery (NB-Name-In)	Private	UDP	Any	137	Any	Any
✓ Network Discovery (Pub-WSD-In)	Private	UDP	Any	3702	LocalSubnet	Any
✓ Network Discovery (SSDP-In)	Private	UDP	Any	1900	LocalSubnet	Any
✓ Network Discovery (UPnP-In)	Private	TCP	Any	2869	Any	Any
✓ Network Discovery (WSD Events-In)	Private	TCP	Any	5357	Any	Any
✓ Network Discovery (WSD EventsSecure-In)	Private	TCP	Any	5358	Any	Any
✓ Network Discovery (WSD-In)	Private	UDP	Any	3702	LocalSubnet	Any
✓ Start	Domain, Private	Any	Any	Any	Any	Any
✓ Start	Domain, Private	Any	Any	Any	Any	Any
✓ Web Management Service (HTTP Traffic-In)	Any	TCP	Any	8172	Any	Any

✓ Windows Management Instrumentation (DCOM-In)	Any	TCP	Any	135	Any	Any
✓ Windows Management Instrumentation (WMI-In)	Any	TCP	Any	Any	Any	Any
✓ Windows Remote Management (HTTP-In)	Public	TCP	Any	5985	LocalSubnet	Any
✓ Windows Remote Management (HTTP-In)	Domain, Private	TCP	Any	5985	Any	Any
✓ Windows Search	Domain, Private	Any	Any	Any	Any	Any
✓ Windows Search	Domain, Private	Any	Any	Any	Any	Any
✓ Workplace or school account	Domain, Private	Any	Any	Any	Any	Any
✓ Workplace or school account	Domain, Private	Any	Any	Any	Any	Any
✓ World Wide Web Services (HTTP Traffic-In)	Any	TCP	Any	80	Any	Any
✓ World Wide Web Services (HTTPS Traffic-In)	Any	TCP	Any	443	Any	Any
✓ World Wide Web Services (QUIC Traffic-In)	Any	UDP	Any	443	Any	Any
✓ Your account	Domain, Private	Any	Any	Any	Any	Any
✓ 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.

82 Windows Firewall Rules

Rule Name	Profile Names	Protocol	Local Addresses	Local Ports	Remote Addresses	Remote Ports
✓ AllJoyn Router (TCP-Out)	Domain, Private	TCP	Any	Any	Any	Any
✓ AllJoyn Router (UDP-Out)	Domain, Private	UDP	Any	Any	Any	Any
✓ Captive Portal Flow	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)	Domain	UDP	Any	Any	Any	Any
✓ Cast to Device streaming server (RTP-Streaming-Out)	Public	UDP	Any	Any	PlayToDevice	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 - Neighbour Discovery Advertisement (ICMPv6-Out)	Any	ICMPv6	Any	RPC	Any	Any
✓ Core Networking - Neighbour 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
✓ Desktop App Web Viewer	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Email and accounts	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Email and accounts	Domain, Private, Public	Any	Any	Any	Any	Any
✓ File and Printer Sharing (Echo Request - ICMPv4-Out)	Domain	ICMPv4	Any	RPC	Any	Any
✓ File and Printer Sharing (Echo Request - ICMPv6-Out)	Domain	ICMPv6	Any	RPC	Any	Any
✓ File and Printer Sharing (LLMNR-UDP-Out)	Domain	UDP	Any	Any	LocalSubnet	5355
✓ File and Printer Sharing (NB-Datagram-Out)	Domain	UDP	Any	Any	Any	138
✓ File and Printer Sharing (NB-Name-Out)	Domain	UDP	Any	Any	Any	137
✓ File and Printer Sharing (NB-Session-Out)	Domain	TCP	Any	Any	Any	139
✓ File and Printer Sharing (SMB-Out)	Domain	TCP	Any	Any	Any	445
✓ mDNS (UDP-Out)	Private	UDP	Any	Any	LocalSubnet	5353
✓ mDNS (UDP-Out)	Public	UDP	Any	Any	LocalSubnet	5353
✓ mDNS (UDP-Out)	Domain	UDP	Any	Any	Any	5353

✓ Microsoft Media Foundation Network Source OUT [TCP ALL]	Any	TCP	Any	Any	LocalSubnet	554, 8554-8558
✓ Narrator	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Narrator	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Network Discovery (LLMNR-UDP-Out)	Private	UDP	Any	Any	LocalSubnet	5355
✓ Network Discovery (NB-Datagram-Out)	Private	UDP	Any	Any	Any	138
✓ Network Discovery (NB-Name-Out)	Private	UDP	Any	Any	Any	137
✓ Network Discovery (Pub WSD-Out)	Private	UDP	Any	Any	LocalSubnet	3702
✓ Network Discovery (SSDP-Out)	Private	UDP	Any	Any	LocalSubnet	1900
✓ Network Discovery (UPnPHost-Out)	Private	TCP	Any	Any	LocalSubnet	2869
✓ Network Discovery (UPnP-Out)	Private	TCP	Any	Any	Any	2869
✓ Network Discovery (WSD Events-Out)	Private	TCP	Any	Any	Any	5357
✓ Network Discovery (WSD EventsSecure-Out)	Private	TCP	Any	Any	Any	5358
✓ Network Discovery (WSD-Out)	Private	UDP	Any	Any	LocalSubnet	3702
✓ Start	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Start	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Windows Default Lock Screen	Domain, Private, Public	Any	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 Defender SmartScreen	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Windows Device Management Certificate Installer (TCP out)	Any	TCP	Any	Any	Any	Any
✓ Windows Device Management Device Enroller (TCP out)	Any	TCP	Any	Any	Any	80, 443
✓ Windows Device Management Enrolment Service (TCP out)	Any	TCP	Any	Any	Any	Any
✓ Windows Device Management Sync Client (TCP out)	Any	TCP	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 Search	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Windows Search	Domain, Private, Public	Any	Any	Any	Any	Any

✓ Windows Security	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, Public	Any	Any	Any	Any	Any
✓ Windows Shell Experience	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Windows Shell Experience	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Workplace or school account	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Workplace or school account	Domain, Private, Public	Any	Any	Any	Any	Any
✓ Your 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.

3 Windows Patches

HotFix ID	Description	Installed By	Installed On
KB5004330	Update		07/08/2021
KB5005104	Update	NT AUTHORITY\SYSTEM	31/08/2021
KB5005111	Update	NT AUTHORITY\SYSTEM	31/08/2021

Windows Update Configuration

Windows Update is a service provided by Microsoft that provides updates for the Windows operating system and installed components. It can be expanded to provide support for other Microsoft software and is then referred to as "Microsoft Update".

The system can be configured either directly or using Group Policy, and updates can be obtained directly from Microsoft over an internet connection or from a Windows Software Update (WSUS) Server installed on the intranet.

General Settings	
Windows Update Mode	Never check for updates (not recommended)
Recommended Updates	Unknown
Include other Microsoft products	False
Registered Services	Windows Update

Advanced	
Allow non-administrators to receive update notifications	Unknown
Automatic Maintenance Enabled	False

Windows Update Server	
Enable Windows Update Server	False

Windows Update History

Windows Update is a service provided by Microsoft that provides updates for the Windows operating system and installed components. This section provides historical information about the updates that have been installed on this machine.

4 History Items

Action Date	Title	Operation	Result
✓ 31 August 2022 16:29:29	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.373.1294.0)	Install	Succeeded
✓ 31 August 2022 16:46:59	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.373.1302.0)	Install	Succeeded
✗ 02 September 2022 10:54:56	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.373.1394.0)	Install	Failed
✓ 31 August 2022 16:36:46	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2205.7)	Install	Succeeded

Software

Provides information about the software and operating system configuration of this machine.

Operating System

Operating System Name	Microsoft Windows Server 2022 Datacenter
Service Pack	[None Installed]

General

Installed Programs	15
Event Logs	9
Environment Variables	21
Scheduled Tasks	6

.NET Framework

The .NET Framework is a software framework developed by Microsoft that runs primarily on Microsoft Windows.

Common Language Runtime (CLR) 1

Name	Status	Service Pack
⚠ .NET Framework 1.0	Not Installed	
⚠ .NET Framework 1.1	Not Installed	

Common Language Runtime (CLR) 2

Name	Status	Service Pack
⚠ .NET Framework 2.0.50727	Not Installed	
⚠ .NET Framework 3.0	Not Installed	
⚠ .NET Framework 3.5	Not Installed	

Common Language Runtime (CLR) 4

Name	Status	Service Pack
✓ .NET Framework 4.0 Client Profile	Installed	
✓ .NET Framework 4.0 Extended	Installed	
✓ .NET Framework 4.5	Installed	
✓ .NET Framework 4.5.1	Installed	
✓ .NET Framework 4.5.2	Installed	
✓ .NET Framework 4.6	Installed	
✓ .NET Framework 4.6.1	Installed	
✓ .NET Framework 4.6.2	Installed	
✓ .NET Framework 4.7	Installed	
✓ .NET Framework 4.7.1	Installed	
✓ .NET Framework 4.7.2	Installed	
✓ .NET Framework 4.8	Installed	

Documented Files

Provides information about the files that have been configured to be documented on the XIA Configuration Client.

1 Files

Display Name	Name	Type	Located
Machine Config (.NET 4)	machine.config	.config	True

Machine Config (.NET 4)

Provides information about the files that have been configured to be documented on the XIA Configuration Client.

File Details

Located	True

General

Full Path	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
File Size	35.14 KB
Creation Date	08 May 2021 09:20:27
Last Accessed	08 May 2021 09:18:32
Last Modified	08 May 2021 09:18:32
File Type	.config
Hidden	False
Read Only	False

Advanced

Encrypted	False
Compressed	False

Security

Owner	NT AUTHORITY\SYSTEM

6 NTFS Permissions

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

0 NTFS Audit Rules

There are no audit rules found.

File Contents

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--
    Please refer to machine.config.comments for a description and
    the default values of each configuration section.

    For a full documentation of the schema please refer to
    http://go.microsoft.com/fwlink/?LinkId=42127

    To improve performance, machine.config should contain only those
    settings that differ from their defaults.
-->
<configuration>
    <configSections>
        <section name="appSettings" type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" restartOnExternalChanges="false" requirePermission="false" />
        <section name="connectionStrings" type="System.Configuration.ConnectionStringsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" requirePermission="false" />
        <section name="mscorlib" type="System.Configuration.IgnoreSection, System.Configuration, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowLocation="false" />
        <section name="runtime"  type="System.Configuration.IgnoreSection, System.Configuration, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowLocation="false" />
        <section name="assemblyBinding"  type="System.Configuration.IgnoreSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowLocation="false" />
        <section name="satelliteassemblies" type="System.Configuration.IgnoreSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowLocation="false" />
        <section name="startup"  type="System.Configuration.IgnoreSection, System.Configuration, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowLocation="false" />
        <section name="system.codedom" type="System.CodeDom.Compiler.CodeDomConfigurationHandler, System, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        <section name="system.data" type="System.Data.Common.DbProviderFactoriesConfigurationHandler, System.Data,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        <section name="system.data.dataset" type="System.Configuration.NameValueFileSectionHandler, System, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" restartOnExternalChanges="false" />
        <section name="system.data.odbc" type="System.Data.Common.DbProviderConfigurationHandler, System.Data, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        <section name="system.data.oledb" type="System.Data.Common.DbProviderConfigurationHandler, System.Data, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        <section name="system.data.oracleclient" type="System.Data.Common.DbProviderConfigurationHandler, System.Data,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        <section name="system.data.sqlclient" type="System.Data.Common.DbProviderConfigurationHandler, System.Data,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        <section name="system.diagnostics" type="System.Diagnostics.SystemDiagnosticsSection, System, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        <section name="system.runtime.remoting" type="System.Configuration.IgnoreSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowLocation="false" />
        <section name="system.windows.forms" type="System.Windows.Forms.WindowsFormsSection, System.Windows.Forms,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        <section name="windows" type="System.Configuration.IgnoreSection, System.Configuration, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowLocation="false" />
        <section name="uri" type="System.Configuration.UriSection, System, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" />
        <sectionGroup name="system.runtime.caching" type="System.Runtime.Caching.Configuration.CachingSectionGroup,
System.Runtime.Caching, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a">
            <section name="memoryCache" type="System.Runtime.Caching.Configuration.MemoryCacheSection, System.Runtime.Caching,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
        </sectionGroup>
        <sectionGroup name="system.xml.serialization" type="System.Xml.Serialization.Configuration.SerializationSectionGroup,
System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
            <section name="schemaImporterExtensions" type="System.Xml.Serialization.Configuration.SchemaImporterExtensionsSection,
System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
            <section name="dateTimeSerialization" type="System.Xml.Serialization.Configuration.DateTimeSerializationSection, System.Xml,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
            <section name="xmlSerializer" type="System.Xml.Serialization.Configuration.XmlSerializerSection, System.Xml, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermission="false" />
        </sectionGroup>
        <sectionGroup name="system.net" type="System.Net.Configuration.NetSectionGroup, System, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089">
            <section name="authenticationModules" type="System.Net.Configuration.AuthenticationModulesSection, System, Version=4.0.0.0,
 Culture=neutral, PublicKeyToken=b77a5c561934e089" />
            <section name="connectionManagement" type="System.Net.Configuration.ConnectionManagementSection, System,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
            <section name="defaultProxy" type="System.Net.Configuration.DefaultProxySection, System, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" />
            <sectionGroup name="mailSettings" type="System.Net.Configuration.MailSettingsSectionGroup, System, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089">
                <section name="smtp" type="System.Net.Configuration.SmtpSection, System, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" />
            </sectionGroup>
            <section name="requestCaching" type="System.Net.Configuration.RequestCachingSection, System, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" />
            <section name="settings" type="System.Net.Configuration.SettingsSection, System, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" />
            <section name="webRequestModules" type="System.Net.Configuration.WebRequestModulesSection, System, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" />
        </sectionGroup>
        <sectionGroup name="system.runtime.serialization" type="System.Runtime.Serialization.Configuration.SerializationSectionGroup,
System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
            <section name="dataContractSerializer" type="System.Runtime.Serialization.Configuration.DataContractSerializerSection,
System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
        </sectionGroup>
        <sectionGroup name="system.serviceModel" type="System.ServiceModel.Configuration.ServiceModelSectionGroup,
System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
            <section name="behaviors" type="System.ServiceModel.Configuration.BehaviorsSection, System.ServiceModel, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="bindings" type="System.ServiceModel.Configuration.BindingsSection, System.ServiceModel, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="client" type="System.ServiceModel.Configuration.ClientSection, System.ServiceModel, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="comContracts" type="System.ServiceModel.Configuration.ComContractsSection, System.ServiceModel,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="commonBehaviors" type="System.ServiceModel.Configuration.CommonBehaviorsSection, System.ServiceModel,
 Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowDefinition="MachineOnly"
allowExeDefinition="MachineOnly"/>
            <section name="diagnostics" type="System.ServiceModel.Configuration.DiagnosticSection, System.ServiceModel,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="extensions" type="System.ServiceModel.Configuration.ExtensionsSection, System.ServiceModel,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="machineSettings" type="System.ServiceModel.Configuration.MachineSettingsSection, SMDiagnostics,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowDefinition="MachineOnly"
allowExeDefinition="MachineOnly"/>
            <section name="protocolMapping" type="System.ServiceModel.Configuration.ProtocolMappingSection, System.ServiceModel,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="serviceHostingEnvironment" type="System.ServiceModel.Configuration.ServiceHostingEnvironmentSection,
System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowDefinition="MachineToApplication"/>
            <section name="services" type="System.ServiceModel.Configuration.ServicesSection, System.ServiceModel, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="standardEndpoints" type="System.ServiceModel.Configuration.StandardEndpointsSection, System.ServiceModel,
 Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="routing" type="System.ServiceModel.Routing.Configuration.RoutingSection, System.ServiceModel.Routing,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
            <section name="tracking" type="System.ServiceModel.Activities.Tracking.Configuration.TrackingSection,
System.ServiceModel.Activities, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        </sectionGroup>
        <sectionGroup name="system.serviceModel.activation"
type="System.ServiceModel.Activation.Configuration.ServiceModelActivationSectionGroup, System.ServiceModel, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089">
            <section name="diagnostics" type="System.ServiceModel.Activation.Configuration.DiagnosticSection, System.ServiceModel,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="net.pipe" type="System.ServiceModel.Activation.Configuration.NetPipeSection, System.ServiceModel,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
            <section name="net.tcp" type="System.ServiceModel.Activation.Configuration.NetTcpSection, System.ServiceModel,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
        </sectionGroup>
        <sectionGroup name="system.transactions" type="System.Transactions.Configuration.TransactionsSectionGroup,
System.Transactions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089, Custom=null">
           <section name="defaultSettings" type="System.Transactions.Configuration.DefaultSettingsSection, System.Transactions,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089, Custom=null" />
           <section name="machineSettings" type="System.Transactions.Configuration.MachineSettingsSection, System.Transactions,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089, Custom=null" allowDefinition="MachineOnly"
allowExeDefinition="MachineOnly"/>
        </sectionGroup>
        <sectionGroup name="system.web" type="System.Web.Configuration.SystemWebSectionGroup, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a">
            <section name="anonymousIdentification" type="System.Web.Configuration.AnonymousIdentificationSection, System.Web,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
            <section name="authentication" type="System.Web.Configuration.AuthenticationSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
            <section name="authorization" type="System.Web.Configuration.AuthorizationSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
            <section name="browserCaps" type="System.Web.Configuration.HttpCapabilitiesSectionHandler, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
            <section name="clientTarget" type="System.Web.Configuration.ClientTargetSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
            <section name="compilation" type="System.Web.Configuration.CompilationSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" requirePermission="false" />
      <section name="customErrors" type="System.Web.Configuration.CustomErrorsSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="deployment" type="System.Web.Configuration.DeploymentSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineOnly" />
      <section name="deviceFilters" type="System.Web.Mobile.DeviceFiltersSection, System.Web.Mobile, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="fullTrustAssemblies" type="System.Web.Configuration.FullTrustAssembliesSection, System.Web,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="globalization" type="System.Web.Configuration.GlobalizationSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="healthMonitoring" type="System.Web.Configuration.HealthMonitoringSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="hostingEnvironment" type="System.Web.Configuration.HostingEnvironmentSection, System.Web,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="httpCookies" type="System.Web.Configuration.HttpCookiesSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="httpHandlers" type="System.Web.Configuration.HttpHandlersSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="httpModules" type="System.Web.Configuration.HttpModulesSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="httpRuntime" type="System.Web.Configuration.HttpRuntimeSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="identity" type="System.Web.Configuration.IdentitySection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="machineKey" type="System.Web.Configuration.MachineKeySection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="membership" type="System.Web.Configuration.MembershipSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="mobileControls" type="System.Web.UI.MobileControls.MobileControlsSection, System.Web.Mobile,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="pages" type="System.Web.Configuration.PagesSection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" requirePermission="false" />
      <section name="partialTrustVisibleAssemblies" type="System.Web.Configuration.PartialTrustVisibleAssembliesSection,
System.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="processModel" type="System.Web.Configuration.ProcessModelSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineOnly" allowLocation="false" />
      <section name="profile" type="System.Web.Configuration.ProfileSection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="protocols" type="System.Web.Configuration.ProtocolsSection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToWebRoot" />
      <section name="roleManager" type="System.Web.Configuration.RoleManagerSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="securityPolicy" type="System.Web.Configuration.SecurityPolicySection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="sessionPageState" type="System.Web.Configuration.SessionPageStateSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="sessionState" type="System.Web.Configuration.SessionStateSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="siteMap" type="System.Web.Configuration.SiteMapSection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="trace" type="System.Web.Configuration.TraceSection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="trust" type="System.Web.Configuration.TrustSection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="urlMappings" type="System.Web.Configuration.UrlMappingsSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      <section name="webControls" type="System.Web.Configuration.WebControlsSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="webParts" type="System.Web.Configuration.WebPartsSection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="webServices" type="System.Web.Services.Configuration.WebServicesSection, System.Web.Services,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <section name="xhtmlConformance" type="System.Web.Configuration.XhtmlConformanceSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <sectionGroup name="caching" type="System.Web.Configuration.SystemWebCachingSectionGroup, System.Web,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a">
        <section name="cache" type="System.Web.Configuration.CacheSection, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
        <section name="outputCache" type="System.Web.Configuration.OutputCacheSection, System.Web, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
        <section name="outputCacheSettings" type="System.Web.Configuration.OutputCacheSettingsSection, System.Web,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
        <section name="sqlCacheDependency" type="System.Web.Configuration.SqlCacheDependencySection, System.Web,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" allowDefinition="MachineToApplication" />
      </sectionGroup>
    </sectionGroup>
    <sectionGroup name="system.web.extensions" type="System.Web.Configuration.SystemWebExtensionsSectionGroup,
System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
            <sectionGroup name="scripting" type="System.Web.Configuration.ScriptingSectionGroup, System.Web.Extensions, 
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
                <section name="scriptResourceHandler" type="System.Web.Configuration.ScriptingScriptResourceHandlerSection, 
System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" requirePermission="false" 
allowDefinition="MachineToApplication"/>
                <sectionGroup name="webServices" type="System.Web.Configuration.ScriptingWebServicesSectionGroup, 
System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
                    <section name="jsonSerialization" type="System.Web.Configuration.ScriptingJsonSerializationSection, 
System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" requirePermission="false" 
allowDefinition="Everywhere" />
                    <section name="profileService" type="System.Web.Configuration.ScriptingProfileServiceSection, System.Web.Extensions, 
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" requirePermission="false" 
allowDefinition="MachineToApplication" />
                    <section name="authenticationService" type="System.Web.Configuration.ScriptingAuthenticationServiceSection, 
System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" requirePermission="false" 
allowDefinition="MachineToApplication" />
                    <section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions, 
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" requirePermission="false" 
allowDefinition="MachineToApplication" />
                </sectionGroup>
            </sectionGroup>
        </sectionGroup>
        <sectionGroup name="system.xaml.hosting" type="System.Xaml.Hosting.Configuration.XamlHostingSectionGroup, 
System.Xaml.Hosting, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
            <section name="httpHandlers" type="System.Xaml.Hosting.Configuration.XamlHostingSection, System.Xaml.Hosting, 
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
        </sectionGroup>
        <section name="system.webServer" type="System.Configuration.IgnoreSection, System.Configuration, Version=4.0.0.0, 
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    </configSections>

    <configProtectedData defaultProvider="RsaProtectedConfigurationProvider">
        <providers>
            <add name="RsaProtectedConfigurationProvider"
            type="System.Configuration.RsaProtectedConfigurationProvider,System.Configuration, Version=4.0.0.0, Culture=neutral, 
PublicKeyToken=b03f5f7f11d50a3a"
            description="Uses RsaCryptoServiceProvider to encrypt and decrypt"
            keyContainerName="NetFrameworkConfigurationKey"
            cspProviderName=""
            useMachineContainer="true"
            useOAEP="true" />

            <add name="DataProtectionConfigurationProvider"
            type="System.Configuration.DpapiProtectedConfigurationProvider,System.Configuration, Version=4.0.0.0, Culture=neutral, 
PublicKeyToken=b03f5f7f11d50a3a"
            description="Uses CryptProtectData and CryptUnProtectData Windows APIs to encrypt and decrypt"
            useMachineProtection="true"
            keyEntropy=""  />
        </providers>
    </configProtectedData>

    <runtime />

    <connectionStrings>
        <add name="LocalSqlServer" connectionString="data source=.\SQLEXPRESS;Integrated 
Security=SSPI;AttachDBFilename=|DataDirectory|aspnetdb.mdf;User Instance=true" providerName="System.Data.SqlClient"/>
    </connectionStrings>

    <system.data>
        <DbProviderFactories />
    </system.data>

    <system.serviceModel>
        <extensions>
            <behaviorExtensions>
                <add name="persistenceProvider" type="System.ServiceModel.Configuration.PersistenceProviderElement, 
System.WorkflowServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
                <add name="workflowRuntime" type="System.ServiceModel.Configuration.WorkflowRuntimeElement, 
System.WorkflowServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
                <add name="enableWebScript" type="System.ServiceModel.Configuration.WebScriptEnablingElement, 
System.ServiceModel.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
                <add name="webHttp" type="System.ServiceModel.Configuration.WebHttpElement, System.ServiceModel.Web, 
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
                <add name="serviceDiscovery" type="System.ServiceModel.Discovery.Configuration.ServiceDiscoveryElement, 
System.ServiceModel.Discovery, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
                <add name="endpointDiscovery" type="System.ServiceModel.Discovery.Configuration.EndpointDiscoveryElement, 
System.ServiceModel.Discovery, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
```

```
        <add name="etwTracking" type="System.ServiceModel.Activities.Configuration.EtwTrackingBehaviorElement,
System.ServiceModel.Activities, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="routing" type="System.ServiceModel.Routing.Configuration.RoutingExtensionElement,
System.ServiceModel.Routing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="soapProcessing" type="System.ServiceModel.Routing.Configuration.SoapProcessingExtensionElement,
System.ServiceModel.Routing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="workflowIdle" type="System.ServiceModel.Activities.Configuration.WorkflowIdleElement,
System.ServiceModel.Activities, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="workflowUnhandledException"
type="System.ServiceModel.Activities.Configuration.WorkflowUnhandledExceptionElement, System.ServiceModel.Activities,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="bufferedReceive" type="System.ServiceModel.Activities.Configuration.BufferedReceiveElement,
System.ServiceModel.Activities, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="sendMessageChannelCache"
type="System.ServiceModel.Activities.Configuration.SendMessageChannelCacheElement, System.ServiceModel.Activities,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="sqlWorkflowInstanceStore"
type="System.ServiceModel.Activities.Configuration.SqlWorkflowInstanceStoreElement, System.ServiceModel.Activities, Version=4.0.0.0,
 Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="workflowInstanceManagement"
type="System.ServiceModel.Activities.Configuration.WorkflowInstanceManagementElement, System.ServiceModel.Activities,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
      </behaviorExtensions>
      <bindingElementExtensions>
        <add name="webMessageEncoding" type="System.ServiceModel.Configuration.WebMessageEncodingElement,
System.ServiceModel.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
        <add name="context" type="System.ServiceModel.Configuration.ContextBindingElementExtensionElement,
System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
        <add name="byteStreamMessageEncoding" type="System.ServiceModel.Configuration.ByteStreamMessageEncodingElement,
System.ServiceModel.Channels, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
        <add name="discoveryClient" type="System.ServiceModel.Discovery.Configuration.DiscoveryClientElement,
System.ServiceModel.Discovery, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
      </bindingElementExtensions>
      <bindingExtensions>
        <add name="wsHttpContextBinding" type="System.ServiceModel.Configuration.WSHttpContextBindingCollectionElement,
System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
        <add name="netTcpContextBinding" type="System.ServiceModel.Configuration.NetTcpContextBindingCollectionElement,
System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
        <add name="webHttpBinding" type="System.ServiceModel.Configuration.WebHttpBindingCollectionElement,
System.ServiceModel.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
        <add name="basicHttpContextBinding" type="System.ServiceModel.Configuration.BasicHttpContextBindingCollectionElement,
System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
      </bindingExtensions>
      <endpointExtensions>
        <add name="dynamicEndpoint" type="System.ServiceModel.Discovery.Configuration.DynamicEndpointCollectionElement,
System.ServiceModel.Discovery, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="discoveryEndpoint" type="System.ServiceModel.Discovery.Configuration.DiscoveryEndpointCollectionElement,
System.ServiceModel.Discovery, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="udpDiscoveryEndpoint"
type="System.ServiceModel.Discovery.Configuration.UdpDiscoveryEndpointCollectionElement, System.ServiceModel.Discovery,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="announcementEndpoint"
type="System.ServiceModel.Discovery.Configuration.AnnouncementEndpointCollectionElement, System.ServiceModel.Discovery,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="udpAnnouncementEndpoint"
type="System.ServiceModel.Discovery.Configuration.UdpAnnouncementEndpointCollectionElement, System.ServiceModel.Discovery,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="workflowControlEndpoint"
type="System.ServiceModel.Activities.Configuration.WorkflowControlEndpointCollectionElement, System.ServiceModel.Activities,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="webHttpEndpoint" type="System.ServiceModel.Configuration.WebHttpEndpointCollectionElement,
System.ServiceModel.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
        <add name="webScriptEndpoint" type="System.ServiceModel.Configuration.WebScriptEndpointCollectionElement,
System.ServiceModel.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
      </endpointExtensions>
    </extensions>
    <client>
      <metadata>
        <policyImporters>
          <extension type="System.ServiceModel.Channels.ContextBindingElementImporter, System.ServiceModel, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089, processorArchitecture=MSIL"/>
        </policyImporters>
        <wsdlImporters>
          <extension type="System.ServiceModel.Channels.ContextBindingElementImporter, System.ServiceModel, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089, processorArchitecture=MSIL"/>
        </wsdlImporters>
      </metadata>
    </client>
    <tracking>
     <profiles>
      <trackingProfile name="">
       <workflow activityDefinitionId="*">
        <workflowInstanceQueries>
         <workflowInstanceQuery>
          <states>
           <state name="*"/>
          </states>
         </workflowInstanceQuery>
        </workflowInstanceQueries>
        <activityStateQueries>
         <activityStateQuery activityName="*">
          <states>
           <state name="Faulted"/>
          </states>
         </activityStateQuery>
        </activityStateQueries>
        <faultPropagationQueries>
         <faultPropagationQuery faultSourceActivityName="*" faultHandlerActivityName="*"/>
        </faultPropagationQueries>
       </workflow>
      </trackingProfile>
     </profiles>
    </tracking>
   </system.serviceModel>
  <system.web>
    <processModel autoConfig="true"/>

    <httpHandlers />

    <membership>
      <providers>
        <add name="AspNetSqlMembershipProvider"
          type="System.Web.Security.SqlMembershipProvider, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a"
          connectionStringName="LocalSqlServer"
          enablePasswordRetrieval="false"
          enablePasswordReset="true"
          requiresQuestionAndAnswer="true"
          applicationName="/"
          requiresUniqueEmail="false"
          passwordFormat="Hashed"
          maxInvalidPasswordAttempts="5"
          minRequiredPasswordLength="7"
          minRequiredNonalphanumericCharacters="1"
          passwordAttemptWindow="10"
          passwordStrengthRegularExpression="" />
      </providers>
    </membership>

    <profile>
      <providers>
        <add name="AspNetSqlProfileProvider" connectionStringName="LocalSqlServer" applicationName="/"
          type="System.Web.Profile.SqlProfileProvider, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" />
      </providers>
    </profile>

    <roleManager>
      <providers>
        <add name="AspNetSqlRoleProvider" connectionStringName="LocalSqlServer" applicationName="/"
          type="System.Web.Security.SqlRoleProvider, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" />
        <add name="AspNetWindowsTokenRoleProvider" applicationName="/"
          type="System.Web.Security.WindowsTokenRoleProvider, System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" />
      </providers>
    </roleManager>
  </system.web>

</configuration>
```

Event Logs

Event logging provides a standard, centralized way for applications and the operating system to record important software and hardware events.

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

9 Event Logs

Name	Type	Maximum File Size	Retention Policy
Application	Administrative	20,480 KB	Overwrite events as needed
Forwarded Events	Operational	20,480 KB	Overwrite events as needed
Hardware Events	Administrative	20,480 KB	Overwrite events as needed
Internet Explorer	Administrative	1,028 KB	Overwrite events as needed
Key Management Service	Administrative	20,480 KB	Overwrite events as needed
Security	Administrative	20,480 KB	Overwrite events as needed
Setup	Operational	1,028 KB	Overwrite events as needed
System	Administrative	20,480 KB	Overwrite events as needed
Windows PowerShell	Administrative	15,360 KB	Overwrite events as needed

Application

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

Event Log Settings

Name	Application
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\Application.evtx
Log Type	Administrative
File Size	2.07 MB
Record Count	3,324

File Access

Created	31 August 2021 22:09:43
Last Accessed	02 September 2022 12:34:16
Last Modified	02 September 2022 12:34:16

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
ℹ Information	02 September 2022 12:33:46	Security-SPP	16384	None	N/A
ℹ Information	02 September 2022 12:33:16	Security-SPP	16394	None	N/A
ℹ Information	02 September 2022 12:25:08	VSS	8224	None	N/A
ℹ Information	02 September 2022 12:18:10	SceCli	1704	None	N/A
ℹ Information	02 September 2022 11:58:56	VSS	8224	None	N/A
ℹ Information	02 September 2022 11:55:25	Security-SPP	16384	None	N/A
ℹ Information	02 September 2022 11:54:56	SceCli	1704	None	N/A
ℹ Information	02 September 2022 11:54:45	Security-SPP	16394	None	N/A
ℹ Information	02 September 2022 11:53:32	Security-SPP	16384	None	N/A
ℹ Information	02 September 2022 11:53:14	VSS	8224	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	31 August 2021 22:09:43
Last Accessed	31 August 2021 22:10:02
Last Modified	31 August 2021 22:10:02

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.

Internet Explorer

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

Event Log Settings

Name	Internet Explorer
Enabled	True
Classic Log	True
Log Path	%SystemRoot%\System32\Winevt\Logs\Internet Explorer.evtx
Log Type	Administrative
File Size	68 KB
Record Count	0

File Access

Created	31 August 2021 22:09:43
Last Accessed	31 August 2021 22:10:02
Last Modified	31 August 2021 22:10:02

Retention

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

Internet Explorer

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	31 August 2021 22:09:43
Last Accessed	31 August 2021 22:10:02
Last Modified	31 August 2021 22:10:02

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	7.07 MB
Record Count	8,226

File Access

Created	31 August 2021 22:09:43
Last Accessed	02 September 2022 12:27:07
Last Modified	02 September 2022 12:27:07

Retention

Maximum File Size	20,480 KB
Retention Policy	Overwrite events as needed

Security

Provides information about the recent events written to this event log.

Most recent 10 entries

Type	Date and Time	Source	Event ID	Task Category	Username
✓ Success Audit	02 September 2022 12:18:10	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 12:18:10	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 12:18:10	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 12:18:10	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 12:18:10	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 12:18:10	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 12:18:10	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 12:18:10	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 11:54:56	Security-Auditing	4719	Audit Policy Change	N/A
✓ Success Audit	02 September 2022 11:54:56	Security-Auditing	4719	Audit Policy Change	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	47

File Access

Created	31 August 2021 22:10:02
Last Accessed	31 August 2022 17:24:31
Last Modified	31 August 2022 17:24:31

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	31 August 2022 16:48:27	Servicing	9	None	NT AUTHORITY\SYSTEM
ⓘ Information	31 August 2022 16:48:23	Servicing	7	None	NT AUTHORITY\SYSTEM
ⓘ Information	31 May 2022 16:17:12	Servicing	9	None	NT AUTHORITY\SYSTEM
ⓘ Information	31 May 2022 16:17:06	Servicing	7	None	NT AUTHORITY\SYSTEM
ⓘ Information	01 September 2021 16:33:47	Servicing	9	None	NT AUTHORITY\SYSTEM
ⓘ Information	01 September 2021 16:33:47	Servicing	9	None	NT AUTHORITY\SYSTEM
ⓘ Information	01 September 2021 16:33:47	Servicing	9	None	NT AUTHORITY\SYSTEM
ⓘ Information	01 September 2021 16:33:47	Servicing	9	None	NT AUTHORITY\SYSTEM
ⓘ Information	01 September 2021 16:33:47	Servicing	9	None	NT AUTHORITY\SYSTEM
ⓘ Information	01 September 2021 16:33:37	Servicing	7	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	3.07 MB
Record Count	6,950

File Access

Created	31 August 2021 22:09:43
Last Accessed	02 September 2022 12:34:18
Last Modified	02 September 2022 12:34:18

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	02 September 2022 12:36:43	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:34:16	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:33:55	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:33:55	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:33:55	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:33:46	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:33:16	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:33:16	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:32:55	Service Control Manager	7036	None	N/A
ⓘ Information	02 September 2022 12:31:57	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	4.07 MB
Record Count	786

File Access

Created	31 August 2021 22:09:43
Last Accessed	02 September 2022 12:32:07
Last Modified	02 September 2022 12:32:07

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	02 September 2022 12:36:56	PowerShell	800	Pipeline Execution Details	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	400	Engine Lifecycle	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	600	Provider Lifecycle	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	600	Provider Lifecycle	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	600	Provider Lifecycle	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	600	Provider Lifecycle	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	600	Provider Lifecycle	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	600	Provider Lifecycle	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	600	Provider Lifecycle	N/A
ⓘ Information	02 September 2022 12:36:56	PowerShell	600	Provider Lifecycle	N/A

Environment Variables

Details the environmental variables found on this machine. Environmental variables can be accessed on Windows Machines by using the SET command at a command prompt. Variables can be user based or SYSTEM variables which are accessible to all users.

21 Environment Variables

Variable Name	Username	Value
%ALLUSERSPROFILE%	<SYSTEM>	C:\ProgramData
%CommonProgramFiles%	<SYSTEM>	C:\Program Files\Common Files
%ComSpec%	<SYSTEM>	C:\Windows\system32\cmd.exe
%DriverData%	<SYSTEM>	C:\Windows\System32\Drivers\DriverData
%NUMBER_OF_PROCESSORS%	<SYSTEM>	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\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\ C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\ C:\Program Files\Microsoft SQL Server\150\Tools\Binn\ C:\Program Files\Microsoft SQL Server\150\DTS\Binn\
%PATHEXT%	<SYSTEM>	.COM .EXE .BAT .CMD .VBS .VBE .JS .JSE .WSF .WSH .MSC
%PROCESSOR_ARCHITECTURE%	<SYSTEM>	AMD64
%PROCESSOR_IDENTIFIER%	<SYSTEM>	Intel64 Family 6 Model 165 Stepping 2, GenuineIntel

%PROCESSOR_LEVEL%	<SYSTEM>	6
%PROCESSOR_REVISION%	<SYSTEM>	a502
%ProgramFiles%	<SYSTEM>	C:\Program Files
%ProgramFiles(x86)%	<SYSTEM>	C:\Program Files (x86)
%PSModulePath%	<SYSTEM>	C:\Program Files\WindowsPowerShell\Modules C:\Windows\system32\WindowsPowerShell\v1.0\Modules C:\Program Files (x86)\Microsoft SQL Server\150\Tools\PowerShell\Modules\
%SystemDrive%	<SYSTEM>	C:
%SystemRoot%	<SYSTEM>	C:\Windows
%TEMP%	<SYSTEM>	C:\Windows\TEMP
%TMP%	<SYSTEM>	C:\Windows\TEMP
%USERNAME%	<SYSTEM>	SYSTEM
%windir%	<SYSTEM>	C:\Windows

Installed Software

Provides information about the programs installed on this Windows machine.

15 Installed Programs

Name	Publisher	Platform	Version	Installation Date
Browser for SQL Server 2019	Microsoft Corporation	32 bit	15.0.2000.5	01 September 2021
Google Chrome	Google LLC	32 bit	104.0.5112.102	31 August 2022
Local Administrator Password Solution	Microsoft Corporation	64 bit	6.2.0.0	31 August 2022
Microsoft Edge	Microsoft Corporation	32 bit	104.0.1293.70	31 August 2022
Microsoft ODBC Driver 17 for SQL Server	Microsoft Corporation	64 bit	17.8.1.1	31 May 2022
Microsoft OLE DB Driver for SQL Server	Microsoft Corporation	64 bit	18.2.3.0	01 September 2021
Microsoft SQL Server 2012 Native Client	Microsoft Corporation	64 bit	11.4.7462.6	01 September 2021
Microsoft SQL Server 2019 (64-bit)	Microsoft Corporation	64 bit		01 September 2021
Microsoft SQL Server 2019 Setup (English)	Microsoft Corporation	64 bit	15.0.4013.40	01 September 2021
Microsoft SQL Server 2019 T-SQL Language Service	Microsoft Corporation	64 bit	15.0.2000.5	01 September 2021
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29913	Microsoft Corporation	32 bit	14.28.29913.0	31 May 2022
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.28.29913	Microsoft Corporation	32 bit	14.28.29913.0	31 May 2022
Microsoft VSS Writer for SQL Server 2019	Microsoft Corporation	64 bit	15.0.2000.5	01 September 2021
VMware Tools	VMware, Inc.	64 bit	11.3.5.18557794	31 May 2022
XIA Configuration Server	CENTREL Solutions	64 bit	14.1.7	31 August 2022

Internet Settings

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

Internet Settings

Internet Explorer Version	11.1.20348.0

System Proxy

Connection Type	Direct Connection

Internet Explorer Enhanced Security

✓ Administrators	True
✓ Users	True

ODBC Configuration

Open Database Connectivity (ODBC) is a standard interface for accessing data in an array of relational and non-relational database management systems (DBMS) without the need for independent software vendors and corporate developers to learn multiple application programming interfaces.

Drivers	23
Data Sources	1

ODBC Drivers

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

23 ODBC Drivers

Name	Platform	ODBC Version	File Version	Filename
Driver da Microsoft para arquivos texto (*.txt; *.csv)	x86	2.50		odbcjt32.dll
Driver do Microsoft Access (*.mdb)	x86	2.50		odbcjt32.dll
Driver do Microsoft dBase (*.dbf)	x86	2.50		odbcjt32.dll
Driver do Microsoft Excel(*.xls)	x86	2.50		odbcjt32.dll
Driver do Microsoft Paradox (*.db)	x86	2.50		odbcjt32.dll
Microsoft Access Driver (*.mdb)	x86	2.50		odbcjt32.dll
Microsoft Access-Treiber (*.mdb)	x86	2.50		odbcjt32.dll
Microsoft dBase Driver (*.dbf)	x86	2.50		odbcjt32.dll
Microsoft dBase-Treiber (*.dbf)	x86	2.50		odbcjt32.dll
Microsoft Excel Driver (*.xls)	x86	2.50		odbcjt32.dll
Microsoft Excel-Treiber (*.xls)	x86	2.50		odbcjt32.dll
Microsoft ODBC for Oracle	x86	2.50		msorcl32.dll
Microsoft Paradox Driver (*.db)	x86	2.50		odbcjt32.dll
Microsoft Paradox-Treiber (*.db)	x86	2.50		odbcjt32.dll
Microsoft Text Driver (*.txt; *.csv)	x86	2.50		odbcjt32.dll
Microsoft Text-Treiber (*.txt; *.csv)	x86	2.50		odbcjt32.dll
ODBC Driver 17 for SQL Server	x64	3.80	2017.178.1.1	msodbcsql17.dll
ODBC Driver 17 for SQL Server	x86	3.80	2017.178.1.1	msodbcsql17.dll
SQL Server	x64	3.50	6.2.20348.1	SQLSRV32.dll
SQL Server	x86	3.50	6.2.20348.1	SQLSRV32.dll
SQL Server Native Client 11.0	x64	3.80	2011.110.7462.6	sqlncli11.dll
SQL Server Native Client 11.0	x86	3.80	2011.110.7462.6	sqlncli11.dll
SQL Server Native Client RDA 11.0	x64	3.80	2011.110.5069.66	sqlnclirda11.dll

Data Sources

A data source, also known as a data source name (DSN) provides the information required to connect to an ODBC compliant data source such as a Microsoft SQL server or Excel Spreadsheet. This information includes the ODBC driver to use, the location of the database file or server and other settings such as the connection credentials.

1 ODBC Data Sources

Name	Platform	Driver Name	Description
SQL Server Data Source	x64	SQL Server	This is a SQL Server data source.

SQL Server Data Source

Provides detailed information about the configuration of this ODBC data source.

General Settings

Description	This is a SQL Server data source.
Driver Name	SQL Server
Driver	C:\Windows\system32\SQLSRV32.dll
Platform	x64
Type Display Name	SQL Server Data Source

SQL Server

Server	XCS-2K22
Authentication Type	Windows NT (integrated) authentication
ANSI Nulls	True
Auto Translate	True
Database	
Database Filename	
Encrypt	False
Failover Server	False
Language	
Quoted Identifiers	True
Use Regional Settings	False

1 Properties

Name	Value
LastUser	sysadmin

Operating System

Provides details about the general operating system configuration.

Operating System

Operating System Name	Microsoft Windows Server 2022 Datacenter
Service Pack	[None Installed]

General

Version	10.0.20348
Operating System Architecture	64-bit
Server Installation Type	Full Server
Build Number	20348
Build Type	Multiprocessor Free
Code Page	1252
Country Code	44
Last BootUp Time	02 September 2022 11:44:14
Install Date	31 August 2021 16:47:11
Locale	0809
MUI Languages	en-GB en-US
Operating System Language	2057
Serial Number	00456-50000-00000-AA529
Windows Directory	C:\Windows
System Directory	C:\Windows\system32

Naming and Role

Domain	test2022.net
Domain Role	Member Server
NetBIOS Name	XCS-2K22
Fully Qualified Domain Name	xcs-2k22.test2022.net

Timezone

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

Registry

Registry Size (Current)	109
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 5.1.20348.202
Runtime Version	4.0.30319.42000
Compatible Versions	1.0 2.0 3.0 4.0 5.0 5.1.20348.202
Machine Execution Policy	Remote Signed
Machine Execution Policy Source	Local

Permissions

Type	Principal	Access
Allow	BUILTIN\Administrators	Full Control (All Operations)
Allow	NT AUTHORITY\INTERACTIVE	Full Control (All Operations)
Allow	BUILTIN\Remote Management Users	Full Control (All Operations)

Audit Rules

Type	Principal	Access
Failure	Everyone	Full Control (All Operations)
Success	Everyone	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.

1 Registry Keys

Display Name	Registry Hive	Located
XIA Configuration Server Setup	HKEY_LOCAL_MACHINE	True

1 Registry Values

Display Name	Value Type	Value	Located
XIA Configuration Server Database Name	REG_SZ	XIAConfiguration	True

XIA Configuration Server Setup

The Windows registry is a hierarchical database that contains configuration data for the operating system, applications, and services. A registry key is a container which stores registry values.

Registry Key

Located	True

Registry Key Properties

Hive	HKEY_LOCAL_MACHINE
Key Name	SOFTWARE\CENTREL Solutions\XIA Configuration Server\Setup

12 Values

Name	Value Type	Data
Account	REG_SZ	NT AUTHORITY\NETWORK SERVICE
AddUserSystemAdministrator	REG_SZ	True
AuthenticationMode	REG_SZ	NETWORKSERVICE
DatabaseInstance	REG_SZ	(local)\SQLEXPRESS
DatabaseName	REG_SZ	XIAConfiguration
Domain	REG_SZ	NT AUTHORITY
InstallDirectory	REG_SZ	C:\Program Files\CENTREL Solutions\XIA Configuration\
OrganizationName	REG_SZ	Demonstration Company
URL	REG_SZ	http://localhost/XIAConfiguration
Username	REG_SZ	NETWORK SERVICE
Version	REG_SZ	14.1.7
VIRDIR	REG_SZ	XIAConfiguration

Security

Owner	NT AUTHORITY\SYSTEM

6 Registry Permissions

Account Name	Inherited	Action	Rights	Applies To
ALL APPLICATION PACKAGES	True	Allow	Read	This key and subkeys
BUILTIN\Administrators	True	Allow	Full Control	This key and subkeys
BUILTIN\Users	True	Allow	Read	This key and subkeys
CREATOR OWNER	True	Allow	Full Control	Subkeys only
NT AUTHORITY\SYSTEM	True	Allow	Full Control	This key and subkeys
? S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479	True	Allow	Read	This key and subkeys

-3232135806-4053264122-3456934681				

0 Registry Audit Rules

There are no audit rules found.

XIA Configuration Server Database Name

The Windows registry is a hierarchical database that contains configuration data for the operating system, applications, and services. A registry value stores an individual value within a registry key.

Registry Value

Located	True

Registry Value Properties

Parent Key	HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Server\Setup
Value Name	DatabaseName
Value	XIAConfiguration
Value Type	REG_SZ

Server Roles and Features

Provides information about the Windows server roles and features such as "DNS Server" enabled on this machine. Server features are found on Windows Server 2008 and above only.

Roles and Features

Feature	Install State
□ .NET Framework 3.5 Features	Available
□ .NET Framework 3.5 (includes .NET 2.0 and 3.0)	Removed
□ HTTP Activation	Available
□ Non-HTTP Activation	Available
☑ .NET Framework 4.8 Features	Installed
☑ .NET Framework 4.8	Installed
☑ ASP.NET 4.8	Installed
☑ WCF Services	Installed
□ HTTP Activation	Available
□ Message Queuing (MSMQ) Activation	Available
□ Named Pipe Activation	Available
□ TCP Activation	Available
☑ TCP Port Sharing	Installed
□ Active Directory Certificate Services	Available
□ Certificate Enrollment Policy Web Service	Available
□ Certificate Enrollment Web Service	Available
□ Certification Authority	Available
□ Certification Authority Web Enrollment	Available
□ Network Device Enrollment Service	Available
□ Online Responder	Available
□ Active Directory Domain Services	Available
□ Active Directory Federation Services	Available
□ Active Directory Lightweight Directory Services	Available
□ Active Directory Rights Management Services	Available
□ Active Directory Rights Management Server	Available
□ Identity Federation Support	Available
□ Background Intelligent Transfer Service (BITS)	Available
□ Compact Server	Available
□ IIS Server Extension	Available
□ BitLocker Drive Encryption	Available
□ BitLocker Network Unlock	Available
□ BranchCache	Available
□ Client for NFS	Available

☐ Containers	Available
☐ Data Center Bridging	Available
☐ Device Health Attestation	Available
☐ DHCP Server	Available
☐ Direct Play	Available
☐ DNS Server	Available
☐ Enhanced Storage	Available
☐ Failover Clustering	Available
☐ Fax Server	Available
☑ File and Storage Services	Installed
☑ File and iSCSI Services	Installed
☐ BranchCache for Network Files	Available
☐ Data Deduplication	Available
☐ DFS Namespaces	Available
☐ DFS Replication	Available
☑ File Server	Installed
☐ File Server Resource Manager	Available
☐ File Server VSS Agent Service	Available
☐ iSCSI Target Server	Available
☐ iSCSI Target Storage Provider (VDS and VSS hardware providers)	Available
☐ Server for NFS	Available
☐ Work Folders	Available
☑ Storage Services	Installed
☑ Group Policy Management	Installed
☐ Host Guardian Hyper-V Support	Available
☐ Host Guardian Service	Available
☐ Hyper-V	Available
☐ I/O Quality of Service	Available
☐ IIS Hostable Web Core	Available
☐ Internet Printing Client	Available
☐ IP Address Management (IPAM) Server	Available
☐ LPR Port Monitor	Available
☐ Management OData IIS Extension	Available
☐ Media Foundation	Available
☐ Message Queuing	Available
☐ Message Queuing DCOM Proxy	Available
☐ Message Queuing Services	Available
☐ Directory Service Integration	Available
☐ HTTP Support	Available
☐ Message Queuing Server	Available

□ Message Queuing Triggers	Available
□ Multicasting Support	Available
□ Routing Service	Available
☑ Microsoft Defender Antivirus	Installed
□ Multipath I/O	Available
□ MultiPoint Connector	Available
□ MultiPoint Connector Services	Available
□ MultiPoint Manager and MultiPoint Dashboard	Available
□ Network Controller	Available
□ Network Load Balancing	Available
□ Network Policy and Access Services	Available
□ Network Virtualization	Available
□ Peer Name Resolution Protocol	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	Available
□ 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
□ SMTP Server 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	Available
□ 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	Available
□ Active Directory module for Windows PowerShell	Available
□ AD DS Tools	Available
□ Active Directory Administrative Center	Available
□ AD DS Snap-Ins and Command-Line Tools	Available
□ AD LDS Snap-Ins and Command-Line Tools	Available
□ DHCP Server Tools	Available
□ DNS Server Tools	Available
□ Fax Server Tools	Available
□ File Services Tools	Available
□ DFS Management Tools	Available
□ 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
□ SMTP Server	Available
□ SNMP Service	Available
□ SNMP WMI Provider	Available
□ Software Load Balancer	Available
□ Storage Migration Service	Available
□ Storage Migration Service Proxy	Available
□ Storage Replica	Available
☑ System Data Archiver	Installed
□ System Insights	Available
□ Telnet Client	Available
□ TFTP Client	Available
□ VM Shielding Tools for Fabric Management	Available
□ Volume Activation Services	Available
☑ Web Server (IIS)	Installed
□ FTP Server	Available
□ FTP Extensibility	Available
□ FTP Service	Available
☑ Management Tools	Installed
□ IIS 6 Management Compatibility	Available
□ IIS 6 Management Console	Available
□ IIS 6 Metabase Compatibility	Available
□ IIS 6 Scripting Tools	Available
□ IIS 6 WMI Compatibility	Available
☑ IIS Management Console	Installed

☑ IIS Management Scripts and Tools	Installed
☑ Management Service	Installed
☑ Web Server	Installed
☑ Application Development	Installed
□ .NET Extensibility 3.5	Available
☑ .NET Extensibility 4.8	Installed
☑ Application Initialization	Installed
□ ASP	Available
□ ASP.NET 3.5	Available
☑ ASP.NET 4.8	Installed
□ CGI	Available
☑ ISAPI Extensions	Installed
☑ ISAPI Filters	Installed
□ Server Side Includes	Available
□ WebSocket Protocol	Available
☑ Common HTTP Features	Installed
☑ Default Document	Installed
☑ Directory Browsing	Installed
☑ HTTP Errors	Installed
□ HTTP Redirection	Available
☑ Static Content	Installed
□ WebDAV Publishing	Available
☑ Health and Diagnostics	Installed
□ Custom Logging	Available
☑ HTTP Logging	Installed
□ Logging Tools	Available
□ ODBC Logging	Available
☑ Request Monitor	Installed
□ Tracing	Available
☑ Performance	Installed
□ Dynamic Content Compression	Available
☑ Static Content Compression	Installed
☑ Security	Installed
□ Basic Authentication	Available
□ Centralized SSL Certificate Support	Available
□ Client Certificate Mapping Authentication	Available
□ Digest Authentication	Available
□ IIS Client Certificate Mapping Authentication	Available
□ IP and Domain Restrictions	Available
☑ Request Filtering	Installed

□ URL Authorization	Available
☑ Windows Authentication	Installed
□ WebDAV Redirector	Available
□ Windows Biometric Framework	Available
□ Windows Deployment Services	Available
□ Deployment Server	Available
□ Transport Server	Available
□ Windows Identity Foundation 3.5	Available
□ Windows Internal Database	Available
☑ Windows PowerShell	Installed
□ Windows PowerShell 2.0 Engine	Removed
☑ Windows PowerShell 5.1	Installed
□ Windows PowerShell Desired State Configuration Service	Available
□ Windows PowerShell Web Access	Available
☑ Windows Process Activation Service	Installed
□ .NET Environment 3.5	Available
☑ Configuration APIs	Installed
☑ Process Model	Installed
□ Windows Search Service	Available
□ Windows Server Backup	Available
□ Windows Server Migration Tools	Available
□ Windows Server Update Services	Available
□ SQL Server Connectivity	Available
□ WID Connectivity	Available
□ WSUS Services	Available
□ Windows Standards-Based Storage Management	Available
□ Windows Subsystem for Linux	Available
□ Windows TIFF IFilter	Available
□ WinRM IIS Extension	Available
□ WINS Server	Available
□ Wireless LAN Service	Available
☑ WoW64 Support	Installed
☑ XPS Viewer	Installed

Startup Commands

Provides information about the commands configured to run at startup for the users of this Windows machine.

bginfo

Command	C:\BGInfo\Bginfo64.exe c:\Bginfo\bg-vm.bgi /SILENT /TIMER:0 /NOLICPROMPT
Location	Common Startup
User	Public

SecurityHealth

Command	%windir%\system32\SecurityHealthSystray.exe
Location	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User	Public

VMware User Process

Command	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
Location	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User	Public

Task Scheduler Library

The Task Scheduler Library automates tasks that perform actions at a specific time or when a certain event occurs and replaces Scheduled Tasks on previous versions of Windows.

6 Scheduled Tasks

Name	Triggers	Account Name
GoogleUpdateTaskMachineCore{722D3B95-1358-4B6A-B6EA-1BA14905F9D7}	Multiple triggers defined	NT AUTHORITY\SYSTEM
GoogleUpdateTaskMachineUA{B5FB06C2-DBE0-4D16-A4FB-4073AED798C6}	At 14:58 every day	NT AUTHORITY\SYSTEM
MicrosoftEdgeUpdateTaskMachineCore	Multiple triggers defined	NT AUTHORITY\SYSTEM
MicrosoftEdgeUpdateTaskMachineUA	At 14:58 every day	NT AUTHORITY\SYSTEM
Process Explorer-TEST2022-sysadmin	At log on of TEST2022\sysadmin	TEST2022\sysadmin
Process Explorer-WIN-K885JAOFNON-Administrator	At log on of XCS-2K22\Administrator	BUILTIN\Administrators

GoogleUpdateTaskMachineCore{722D3B95-1358-4B6A-B6EA-1BA14905F9D7}

Keeps your Google software up to date. If this task is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This task uninstalls itself when there is no Google software using it.

General

Name	GoogleUpdateTaskMachineCore{722D3B95-1358-4B6A-B6EA-1BA14905F9D7}
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)\Google\Update\GoogleUpdate.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 14:58 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

GoogleUpdateTaskMachineUA{B5FB06C2-DBE0-4D16-A4FB-4073AED798C6}

Keeps your Google software up to date. If this task is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This task uninstalls itself when there is no Google software using it.

General

Name	GoogleUpdateTaskMachineUA{B5FB06C2-DBE0-4D16-A4FB-4073AED798C6}
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)\Google\Update\GoogleUpdate.exe
Arguments	/ua /installsource scheduler
Working Directory	

On specified schedule

Summary	At 14:58 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

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
Task Path	\
Author	
Enabled	True
Hidden	False
Version	Windows Vista™ or Windows Server™ 2008

Security

Account Name	NT AUTHORITY\SYSTEM
Logon Type	Run whether user is logged on or not (service).
Use Highest Privileges	True

Settings

Allow Task To Be Run On Demand	True
Run After Missed Scheduled Start	True
Task Failure Restart	Do not restart
Execution Time Limit	Stop the task if it runs longer than 3 days
Force Terminate Tasks	True
Delete Expired Task	Do not delete
Multiple Instance Action	Do not start a new instance

Conditions

Idle Duration	Do not wait for the computer to become idle
Disallow Start On Batteries	False
Wake Computer To Run Task	False
Network Requirement	None

Execute Action

Command	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
Arguments	/c
Working Directory	

At log on

Summary	At log on of any user
Delay Task	No delay
Repetition	No repetition
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Activate Task	[Not Configured]
Activate Task (Synchronize)	False
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

On specified schedule

Summary	At 15:28 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

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
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 14:58 every day
Delay Task	No delay
Repetition	Repeat the task every 1 hour for 1 day
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

Process Explorer-TEST2022-sysadmin

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

General

Name	Process Explorer-TEST2022-sysadmin
Task Path	\
Author	Process Explorer
Enabled	True
Hidden	False
Version	Windows Vista™ or Windows Server™ 2008

Security

Account Name	TEST2022\sysadmin
Logon Type	Run only when a user is logged on.
Use Highest Privileges	False

Settings

Allow Task To Be Run On Demand	True
Run After Missed Scheduled Start	True
Task Failure Restart	Do not restart
Execution Time Limit	Stop the task if it runs longer than 3 days
Force Terminate Tasks	True
Delete Expired Task	Do not delete
Multiple Instance Action	Do not start a new instance

Conditions

Idle Duration	Do not wait for the computer to become idle
Disallow Start On Batteries	False
Wake Computer To Run Task	False
Network Requirement	None

Execute Action

Command	"C:\PROCESSEXPLORER\PROCEXP64.EXE"
Arguments	/t
Working Directory	

At log on

Summary	At log on of TEST2022\sysadmin
Delay Task	No delay
Repetition	No repetition
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Activate Task	[Not Configured]
Activate Task (Synchronize)	False
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

Process Explorer-WIN-K885JAOFNON-Administrator

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

General

Name	Process Explorer-WIN-K885JAOFNON-Administrator
Task Path	\
Author	Process Explorer
Enabled	True
Hidden	False
Version	Windows Vista™ or Windows Server™ 2008

Security

Account Name	BUILTIN\Administrators
Logon Type	Run only when a user is logged on.
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:\PROCESSEXPLORER\PROCEXP64.EXE"
Arguments	/t
Working Directory	

At log on

Summary	At log on of XCS-2K22\Administrator
Delay Task	No delay
Repetition	No repetition
Stop Tasks At Repetition Duration End	False
Execution Time Limit	No execution time limit
Activate Task	[Not Configured]
Activate Task (Synchronize)	False
Task Expiry	Does not expire
Expire Task (Synchronize)	False
Enabled	True

Windows Remote Management (WinRM)

Windows Remote Management (WinRM) is the Microsoft implementation of the WS-MAN management protocol, and the underlying communication technology used by PowerShell remoting.

Service Settings

Allow Remote Server Management	True
Allow Unencrypted Traffic	False
Channel Binding Token Hardening	Relaxed
Disallow Storing RunAs Credentials	False
IPv4 Filter	*
IPv6 Filter	*
Started	True
Use HTTP Compatibility Listener	False
Use HTTPS Compatibility Listener	False
Version	10.0.20348.1

Service Authentication Settings

Allow Basic Authentication	False
Allow CredSSP Authentication	False
Allow Kerberos Authentication	True
Allow Negotiate Authentication	True

Listener Listener_1084132640

Enabled	True
Address	*
Port	5985
Protocol	HTTP
URI Prefix	wsman

Client Settings

Allow Unencrypted Traffic	False
Default HTTP Port	5985
Default HTTPS Port	5986
Trusted Hosts	*
Trusted Hosts Source	Configured Locally

Client Authentication Settings

Allow Basic Authentication	True
Allow CredSSP Authentication	False
Allow Digest Authentication	True
Allow Kerberos Authentication	True
Allow Negotiate Authentication	True

Windows Remote Shell

Allow Remote Shell Access	True
Allow Remote Shell Access Source	Not Defined
Idle Timeout (ms)	7,200,000
Maximum Concurrent Users	2,147,483,647
Maximum Memory Per Shell (MB)	2,147,483,647
Maximum Processes Per Shell	2,147,483,647
Maximum Shells Per User	2,147,483,647

Windows Services

Displays the configuration of the Windows services on this machine

227 Windows Services

Display Name	Start Mode	Account Name
ActiveX Installer (AxInstSV)	Disabled	LocalSystem
AllJoyn Router Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
App Readiness	Manual	LocalSystem
Application Host Helper Service	Automatic	localSystem
Application Identity	Manual (Trigger Start)	NT Authority\LocalService
Application Information	Manual (Trigger Start)	LocalSystem
Application Layer Gateway Service	Manual	NT AUTHORITY\LocalService
Application Management	Manual	LocalSystem
AppX Deployment Service (AppXSVC)	Manual (Trigger Start)	LocalSystem
ASP.NET State Service	Manual	NT AUTHORITY\NetworkService
Auto Time Zone Updater	Disabled	NT AUTHORITY\LocalService
AzureAttestService	Automatic	LocalSystem
Background Intelligent Transfer Service	Manual	LocalSystem
Background Tasks Infrastructure Service	Automatic	LocalSystem
Base Filtering Engine	Automatic	NT AUTHORITY\LocalService
Bluetooth Support Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
Capability Access Manager Service	Manual	LocalSystem
CaptureService_526cb	Manual	
cbdhsvc_526cb	Automatic	
CDPUserSvc_526cb	Automatic	

Certificate Propagation	Manual (Trigger Start)	LocalSystem
Client Licence Service (ClipSVC)	Manual (Trigger Start)	LocalSystem
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 User Experiences and Telemetry	Automatic	LocalSystem
ConsentUxUserSvc_526cb	Manual	
CoreMessaging	Automatic	NT AUTHORITY\LocalService
Credential Manager	Manual	LocalSystem
CredentialEnrollmentManagerUserSvc_526cb	Manual	
Cryptographic Services	Automatic	NT Authority\NetworkService
Data Sharing Service	Manual (Trigger Start)	LocalSystem
DCOM Server Process Launcher	Automatic	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	Disabled	LocalSystem
Device Setup Manager	Manual (Trigger Start)	LocalSystem
DeviceAssociationBrokerSvc_526cb	Manual	
DevicePickerUserSvc_526cb	Disabled	
DevicesFlowUserSvc_526cb	Manual	
DevQuery Background Discovery Broker	Manual (Trigger Start)	LocalSystem
DHCP Client	Automatic	NT Authority\LocalService
Diagnostic Policy Service	Automatic (Delayed Start)	NT AUTHORITY\LocalService

Diagnostic Service Host	Manual	NT AUTHORITY\LocalService
Diagnostic System Host	Manual	LocalSystem
Display Policy Service	Automatic (Delayed Start)	NT AUTHORITY\LocalService
Distributed Link Tracking Client	Automatic	LocalSystem
Distributed Transaction Coordinator	Automatic (Delayed Start)	NT AUTHORITY\NetworkService
DNS Client	Automatic (Trigger Start)	NT AUTHORITY\NetworkService
Downloaded Maps Manager	Disabled	NT AUTHORITY\NetworkService
Embedded Mode	Manual (Trigger Start)	LocalSystem
Encrypting File System (EFS)	Manual (Trigger Start)	LocalSystem
Enterprise App Management Service	Manual	LocalSystem
Extensible Authentication Protocol	Manual	localSystem
Function Discovery Provider Host	Manual	NT AUTHORITY\LocalService
Function Discovery Resource Publication	Manual (Trigger Start)	NT AUTHORITY\LocalService
Geolocation Service	Disabled	LocalSystem
Google Chrome Elevation Service (GoogleChromeElevationService)	Manual	LocalSystem
Google Update Service (gupdate)	Automatic (Delayed Start)	LocalSystem
Google Update Service (gupdatem)	Manual	LocalSystem
GraphicsPerfSvc	Disabled	LocalSystem
Group Policy Client	Automatic (Trigger Start)	LocalSystem
Human Interface Device Service	Manual (Trigger Start)	LocalSystem
HV Host Service	Manual (Trigger Start)	LocalSystem
Hyper-V Data Exchange Service	Manual (Trigger Start)	LocalSystem
Hyper-V Guest Service Interface	Manual (Trigger Start)	LocalSystem
Hyper-V Guest Shutdown Service	Manual (Trigger Start)	LocalSystem
Hyper-V Heartbeat Service	Manual (Trigger Start)	LocalSystem
Hyper-V PowerShell Direct Service	Manual (Trigger Start)	LocalSystem

Hyper-V Time Synchronization Service	Manual (Trigger Start)	NT AUTHORITY\LocalService
Hyper-V Volume Shadow Copy Requestor	Manual (Trigger Start)	LocalSystem
IKE and AuthIP IPsec Keying Modules	Manual (Trigger Start)	LocalSystem
Internet Connection Sharing (ICS)	Disabled	LocalSystem
IP Helper	Automatic	LocalSystem
IPsec Policy Agent	Manual (Trigger Start)	NT Authority\NetworkService
KDC Proxy Server service (KPS)	Manual	NT AUTHORITY\NetworkService
KtmRm for Distributed Transaction Coordinator	Manual (Trigger Start)	NT AUTHORITY\NetworkService
Link-Layer Topology Discovery Mapper	Disabled	NT AUTHORITY\LocalService
Local Session Manager	Automatic	LocalSystem
McpManagementService	Manual	LocalSystem
Microsoft (R) Diagnostics Hub Standard Collector Service	Manual	LocalSystem
Microsoft Account Sign-in Assistant	Manual (Trigger Start)	LocalSystem
Microsoft App-V Client	Disabled	LocalSystem
Microsoft Defender Antivirus Network Inspection Service	Manual	NT AUTHORITY\LocalService
Microsoft Defender Antivirus Service	Automatic	LocalSystem
Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)	Manual	LocalSystem
Microsoft Edge Update Service (edgeupdate)	Automatic (Delayed Start, Trigger Start)	LocalSystem
Microsoft Edge Update Service (edgeupdatem)	Manual (Trigger Start)	LocalSystem
Microsoft iSCSI Initiator Service	Manual	LocalSystem
Microsoft 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
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\LocalService
Network Location Awareness	Automatic	NT AUTHORITY\NetworkService
Network Setup Service	Manual (Trigger Start)	LocalSystem
Network Store Interface Service	Automatic	NT Authority\LocalService
Offline Files	Disabled	LocalSystem
OpenSSH Authentication Agent	Disabled	LocalSystem
Optimise drives	Manual	localSystem
Payments and NFC/SE Manager	Disabled	NT AUTHORITY\LocalService
Performance Counter DLL Host	Manual	NT AUTHORITY\LocalService
Performance Logs & Alerts	Manual	NT AUTHORITY\LocalService
PimIndexMaintenanceSvc_526cb	Manual	
Plug and Play	Manual	LocalSystem
Portable Device Enumerator Service	Manual (Trigger Start)	LocalSystem
Power	Automatic	LocalSystem
Print Spooler	Automatic	LocalSystem
Printer Extensions and Notifications	Manual	LocalSystem
PrintWorkflowUserSvc_526cb	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	Disabled	NT AUTHORITY\LocalService
Remote Access Auto Connection Manager	Manual	localSystem

Remote Access Connection Manager	Automatic	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 Log-on	Manual	LocalSystem
Secure Socket Tunneling Protocol Service	Manual	NT Authority\LocalService
Security Accounts Manager	Automatic	LocalSystem
Sensor Data Service	Disabled	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	Disabled	LocalSystem
Smart Card Removal Policy	Manual	LocalSystem
SNMP Trap	Manual	NT AUTHORITY\LocalService
Software Protection	Automatic (Delayed Start, Trigger Start)	NT AUTHORITY\NetworkService
Special Administration Console Helper	Manual	LocalSystem
Spot Verifier	Manual (Trigger Start)	LocalSystem

SQL Server (SQLEXPRESS)	Automatic	NT Service\MSSQL$SQLEXPRESS
SQL Server Agent (SQLEXPRESS)	Disabled	NT AUTHORITY\NETWORKSERVICE
SQL Server Browser	Disabled	NT AUTHORITY\LOCALSERVICE
SQL Server CEIP service (SQLEXPRESS)	Automatic	NT Service\SQLTELEMETRY$SQLEXPRESS
SQL Server VSS Writer	Automatic	LocalSystem
SSDP Discovery	Disabled	NT AUTHORITY\LocalService
State Repository Service	Automatic	LocalSystem
Still Image Acquisition Events	Manual	LocalSystem
Storage Service	Automatic (Delayed Start, Trigger Start)	LocalSystem
Storage Tiers Management	Manual	localSystem
SysMain	Automatic	LocalSystem
System Event Notification Service	Automatic	LocalSystem
System Events Broker	Automatic (Trigger Start)	LocalSystem
System Guard Runtime Monitor Broker	Manual (Trigger Start)	LocalSystem
Task Scheduler	Automatic	LocalSystem
TCP/IP NetBIOS Helper	Manual (Trigger Start)	NT AUTHORITY\LocalService
Telephony	Manual	NT AUTHORITY\NetworkService
Themes	Automatic	LocalSystem
Time Broker	Manual (Trigger Start)	NT AUTHORITY\LocalService
Touch Keyboard and Handwriting Panel Service	Manual (Trigger Start)	LocalSystem
UdkUserSvc_526cb	Manual	
UnistoreSvc_526cb	Manual	
Update Orchestrator Service	Automatic (Delayed Start)	LocalSystem
UPnP Device Host	Disabled	NT AUTHORITY\LocalService
User Access Logging Service	Automatic (Delayed Start)	LocalSystem
User Experience Virtualization Service	Disabled	LocalSystem

User Manager	Automatic (Trigger Start)	LocalSystem
User Profile Service	Automatic	LocalSystem
UserDataSvc_526cb	Manual	
Virtual Disk	Manual	LocalSystem
VMware Alias Manager and Ticket Service	Automatic	LocalSystem
VMware Snapshot Provider	Manual	LocalSystem
VMware SVGA Helper Service	Automatic	LocalSystem
VMware Tools	Automatic	LocalSystem
Volume Shadow Copy	Manual	LocalSystem
W3C Logging Service	Manual	localSystem
WalletService	Disabled	LocalSystem
Warp JIT Service	Manual (Trigger Start)	NT Authority\LocalService
Web Account Manager	Manual	LocalSystem
Web Management Service	Manual	NT AUTHORITY\LocalService
Windows Audio	Manual	NT AUTHORITY\LocalService
Windows Audio Endpoint Builder	Manual	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 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	NT Authority\LocalService
Windows Insider Service	Disabled	LocalSystem
Windows Installer	Manual	LocalSystem
Windows License Manager Service	Manual (Trigger Start)	NT Authority\LocalService
Windows Management Instrumentation	Automatic	localSystem
Windows Media Player Network Sharing Service	Manual	NT AUTHORITY\NetworkService
Windows Modules Installer	Manual	localSystem
Windows Process Activation Service	Manual	localSystem
Windows Push Notifications System Service	Automatic	LocalSystem
Windows PushToInstall Service	Disabled	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
Windows Update Medic Service	Manual	LocalSystem
WinHTTP Web Proxy Auto-Discovery Service	Manual	NT AUTHORITY\LocalService
Wired AutoConfig	Manual	localSystem
WMI Performance Adapter	Manual	localSystem
Workstation	Automatic	NT AUTHORITY\NetworkService
World Wide Web Publishing Service	Automatic	localSystem
WpnUserService_526cb	Automatic	
XIA Configuration Scheduler	Automatic	NT AUTHORITY\NETWORK SERVICE
XIA Configuration Service	Automatic	TEST2022\sysadmin

Windows Time

The Windows Time service, also known as W32Time, synchronizes the date on Windows computers. Time synchronization is critical for the proper operation of many Windows services and line-of-business applications.

Active Directory

Domain Role	Member Server

Service Information

Start Mode	Automatic (Trigger Start)
Service State	Running

Global Settings

MaxNegPhaseCorrection	4,294,967,295
MaxPosPhaseCorrection	4,294,967,295
VMIC Provider Status	Enabled

Client Settings

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

Server Settings

Enabled	False

Support Provisions

This section provides information about the support provisions associated with this item.

2 Support Provisions

Name	Relationship Type	Hours	Start Date	Expiry Date
Network Support	Technical Support	8am-5pm	01 September 2022	01 September 2032
Hardware Warranty	Hardware Maintenance	9-5pm Mon-Fri	01 September 2022	01 September 2032

Network Support

This section provides information about the support provisions associated with this item.

Relationship Information

Relationship Type	Technical Support

Support Provision Details

Support Hours	8am-5pm
Reference Number	53964
Self Service Web Site	http://www.contoso.com
Email Address	support@contoso.com
Telephone Number	+44 (0)1234 123456

Validity Period

Start Date	01 September 2022
Expiry Date	01 September 2032

Hardware Warranty

This section provides information about the support provisions associated with this item.

Relationship Information

Relationship Type	Hardware Maintenance

Support Provision Details

Support Hours	9-5pm Mon-Fri
Reference Number	633673356
Self Service Web Site	http://www.hpwarranty.com/logcall.aspx
Email Address	support@hpwarranty.com
Telephone Number	+44 (0)1235 589123

Validity Period

Start Date	01 September 2022
Expiry Date	01 September 2032

Version History

The version history displays the changes that have been made to the documentation of this item over time - either automatically when a change has been detected, or manually by users of the system.

2 versions

Version	Username	Date	Time	Description
1.01	TEST2022\sysadmin	02 September 2022	13:03	Added primary owner and hardware information.
1.00	TEST2022\sysadmin	02 September 2022	12:44	