

Windows Machine Report

XCS-2K22



Contoso Foods Inc.



CONTOSO FOODS

Date	02 September 2022 13:06:23
Author	TEST2022\sysadmin
Version	1.01
Product	XIA Configuration Server [14.1.7.0]

Table of Contents

Disclaimer	15
Windows Server Information	16
Client Information	17
Relationships	18
Relationship Map	19
Management Summary	20
Compliance Benchmarks	21
Windows Basic Compliance Benchmark [5.0.0.0]	22
Location	37
Hardware	38
BIOS Information	39
CD-ROM and DVD-ROM Drives	40
Disk Drives	41
[0] VMware Virtual SATA Hard Drive	42
[1] VMware Virtual NVMe Disk	43
Disk Shelves	45
Disk Shelf 01	46
Volumes	47
C:	48
E: (ReFS Volume)	49
EFI System Partition (a4843695-894b-4c80-b1fe-ebc21feb01fc)	50
Recovery Partition (462dd327-6aac-4b83-a6e9-7bfa44242e04)	51
Devices	52
Batteries	59
Computer	60
Disk drives	61

Display adapters	62
DVD/CD-ROM drives	63
Human Interface Devices	64
IDE ATA/ATAPI controllers	65
Keyboards	67
Mice and other pointing devices	68
Monitors	70
Network adapters	71
Ports (COM & LPT)	77
Print queues	78
Processors	80
Software devices	81
Sound, video and game controllers	82
Storage controllers	83
Storage volumes	84
System devices	87
Universal Serial Bus controllers	145
Physical Memory	149
Printers	150
Microsoft XPS Document Writer	151
Microsoft Print to PDF	152
Processors	153
Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	154
Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz	155
Tape Libraries	156
Tape Library 1	157
Video Controllers	158
Networking	159
Hosts File	160

Network Adapters	162
6to4 Adapter	163
Ethernet (Kernel Debugger)	164
Ethernet0	165
Local Area Connection* 1	168
Local Area Connection* 2	169
Local Area Connection* 3	170
Local Area Connection* 4	171
Local Area Connection* 5	172
Local Area Connection* 6	173
Local Area Connection* 7	174
Local Area Connection* 8	175
Local Area Connection* 9	176
Microsoft IP-HTTPS Platform Interface	177
Teredo Tunneling Pseudo-Interface	178
Network Load Balancing	179
IPv4 Routing Table	180
Remote Assistance	181
Remote Desktop	182
SNMP Configuration	183
Shares	184
ADMIN\$	185
C\$	186
E\$	187
IPC\$	188
Shared Folder	189
Security	190
Advanced Audit Policy	191
Audit Policy	194

Certificate Stores	195
Intermediate Certification Authorities	196
Microsoft Windows Hardware Compatibility	197
Root Agency	198
www.verisign.com/CPS Incorporation by Reference. LIABILITY LIMITED BY OUR TERMS OF SERVICE. ©1997 VeriSign	199
Personal	200
WMSvc-SHA2-XCS-2K22	201
Third-Party Root Certification Authorities	202
AAA Certificate Services	203
Baltimore CyberTrust Root	204
Class 3 Public Primary Certification Authority	205
DigiCert Assured ID Root CA	206
DigiCert Global Root CA	207
DigiCert Global Root G2	208
DigiCert High Assurance EV Root CA	209
DigiCert Trusted Root G4	210
DST Root CA X3	211
Entrust Root Certification Authority - G2	212
GlobalSign	213
GlobalSign Root CA	214
Go Daddy Class 2 Certification Authority	215
QuoVadis Root CA 2 G3	216
Starfield Class 2 Certification Authority	217
VeriSign Class 3 Public Primary Certification Authority - G5	218
Trusted People	219
Trusted Publisher	220
Trusted Root Certification Authorities	221
Copyright (c) 1997 Microsoft Corp.	222
Microsoft Authenticode(tm) Root Authority	223

Microsoft ECC Product Root Certificate Authority 2018	224
Microsoft ECC TS Root Certificate Authority 2018	225
Microsoft Root Authority	226
Microsoft Root Certificate Authority	227
Microsoft Root Certificate Authority 2010	228
Microsoft Root Certificate Authority 2011	229
Microsoft Time Stamp Root Certificate Authority 2014	230
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	231
Symantec Enterprise Mobile Root for Microsoft	232
Thawte Timestamping CA	233
WMSvc-SHA2-XCS-2K22	234
Web Hosting	235
Local Account Policies	236
LAPS Settings	237
Local Users	238
Administrator	239
DefaultAccount	240
Guest	241
WDAGUtilityAccount	242
Local Groups	243
Microsoft Defender	247
Security Options	248
User Rights Assignment	258
Windows Firewall	262
Domain Profile	263
Private Profile	264
Public Profile	265
Inbound Rules	266
** Dynamic TCP incoming	270

** TCP Port 1433	271
** UDP Port 1434	272
AllJoyn Router (TCP-In)	273
AllJoyn Router (UDP-In)	274
Cast to Device functionality (qWave-TCP-In)	275
Cast to Device functionality (qWave-UDP-In)	276
Cast to Device SSDP Discovery (UDP-In)	277
Cast to Device streaming server (HTTP-Streaming-In)	278
Cast to Device streaming server (HTTP-Streaming-In)	279
Cast to Device streaming server (HTTP-Streaming-In)	280
Cast to Device streaming server (RTCP-Streaming-In)	281
Cast to Device streaming server (RTCP-Streaming-In)	282
Cast to Device streaming server (RTCP-Streaming-In)	283
Cast to Device streaming server (RTSP-Streaming-In)	284
Cast to Device streaming server (RTSP-Streaming-In)	285
Cast to Device streaming server (RTSP-Streaming-In)	286
Cast to Device UPnP Events (TCP-In)	287
Core Networking - Destination Unreachable (ICMPv6-In)	288
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)	289
Core Networking - Dynamic Host Configuration Protocol (DHCP-In)	290
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)	291
Core Networking - Internet Group Management Protocol (IGMP-In)	292
Core Networking - IPHTTPS (TCP-In)	293
Core Networking - IPv6 (IPv6-In)	294
Core Networking - Multicast Listener Done (ICMPv6-In)	295
Core Networking - Multicast Listener Query (ICMPv6-In)	296
Core Networking - Multicast Listener Report (ICMPv6-In)	297
Core Networking - Multicast Listener Report v2 (ICMPv6-In)	298
Core Networking - Neighbour Discovery Advertisement (ICMPv6-In)	299

Core Networking - Neighbour Discovery Solicitation (ICMPv6-In)	300
Core Networking - Packet Too Big (ICMPv6-In)	301
Core Networking - Parameter Problem (ICMPv6-In)	302
Core Networking - Router Advertisement (ICMPv6-In)	303
Core Networking - Router Solicitation (ICMPv6-In)	304
Core Networking - Teredo (UDP-In)	305
Core Networking - Time Exceeded (ICMPv6-In)	306
Delivery Optimization (TCP-In)	307
Delivery Optimization (UDP-In)	308
Desktop App Web Viewer	309
Desktop App Web Viewer	310
DIAL protocol server (HTTP-In)	311
DIAL protocol server (HTTP-In)	312
File and Printer Sharing (Echo Request - ICMPv4-In)	313
File and Printer Sharing (Echo Request - ICMPv6-In)	314
File and Printer Sharing (LLMNR-UDP-In)	315
File and Printer Sharing (NB-Datagram-In)	316
File and Printer Sharing (NB-Name-In)	317
File and Printer Sharing (NB-Session-In)	318
File and Printer Sharing (SMB-In)	319
File and Printer Sharing (Spooler Service - RPC)	320
File and Printer Sharing (Spooler Service - RPC-EPMAP)	321
File Server Remote Management (DCOM-In)	322
File Server Remote Management (SMB-In)	323
File Server Remote Management (WMI-In)	324
Google Chrome (mDNS-In)	325
mDNS (UDP-In)	326
mDNS (UDP-In)	327
mDNS (UDP-In)	328

Microsoft Edge (mDNS-In)	329
Microsoft Media Foundation Network Source IN [TCP 554]	330
Microsoft Media Foundation Network Source IN [UDP 5004-5009]	331
Network Discovery (LLMNR-UDP-In)	332
Network Discovery (NB-Datagram-In)	333
Network Discovery (NB-Name-In)	334
Network Discovery (Pub-WSD-In)	335
Network Discovery (SSDP-In)	336
Network Discovery (UPnP-In)	337
Network Discovery (WSD Events-In)	338
Network Discovery (WSD EventsSecure-In)	339
Network Discovery (WSD-In)	340
Start	341
Start	342
Web Management Service (HTTP Traffic-In)	343
Windows Management Instrumentation (DCOM-In)	344
Windows Management Instrumentation (WMI-In)	345
Windows Remote Management (HTTP-In)	346
Windows Remote Management (HTTP-In)	347
Windows Search	348
Windows Search	349
Workplace or school account	350
Workplace or school account	351
World Wide Web Services (HTTP Traffic-In)	352
World Wide Web Services (HTTPS Traffic-In)	353
World Wide Web Services (QUIC Traffic-In)	354
Your account	355
Your account	356
Outbound Rules	357

AllJoyn Router (TCP-Out)	361
AllJoyn Router (UDP-Out)	362
Captive Portal Flow	363
Captive Portal Flow	364
Cast to Device functionality (qWave-TCP-Out)	365
Cast to Device functionality (qWave-UDP-Out)	366
Cast to Device streaming server (RTP-Streaming-Out)	367
Cast to Device streaming server (RTP-Streaming-Out)	368
Cast to Device streaming server (RTP-Streaming-Out)	369
Connected User Experiences and Telemetry	370
Core Networking - DNS (UDP-Out)	371
Core Networking - Dynamic Host Configuration Protocol (DHCP-Out)	372
Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPV6-Out)	373
Core Networking - Group Policy (LSASS-Out)	374
Core Networking - Group Policy (NP-Out)	375
Core Networking - Group Policy (TCP-Out)	376
Core Networking - Internet Group Management Protocol (IGMP-Out)	377
Core Networking - IPHTTPS (TCP-Out)	378
Core Networking - IPv6 (IPv6-Out)	379
Core Networking - Multicast Listener Done (ICMPv6-Out)	380
Core Networking - Multicast Listener Query (ICMPv6-Out)	381
Core Networking - Multicast Listener Report (ICMPv6-Out)	382
Core Networking - Multicast Listener Report v2 (ICMPv6-Out)	383
Core Networking - Neighbour Discovery Advertisement (ICMPv6-Out)	384
Core Networking - Neighbour Discovery Solicitation (ICMPv6-Out)	385
Core Networking - Packet Too Big (ICMPv6-Out)	386
Core Networking - Parameter Problem (ICMPv6-Out)	387
Core Networking - Router Advertisement (ICMPv6-Out)	388
Core Networking - Router Solicitation (ICMPv6-Out)	389

Core Networking - Teredo (UDP-Out)	390
Core Networking - Time Exceeded (ICMPv6-Out)	391
Desktop App Web Viewer	392
Desktop App Web Viewer	393
Email and accounts	394
Email and accounts	395
File and Printer Sharing (Echo Request - ICMPv4-Out)	396
File and Printer Sharing (Echo Request - ICMPv6-Out)	397
File and Printer Sharing (LLMNR-UDP-Out)	398
File and Printer Sharing (NB-Datagram-Out)	399
File and Printer Sharing (NB-Name-Out)	400
File and Printer Sharing (NB-Session-Out)	401
File and Printer Sharing (SMB-Out)	402
mDNS (UDP-Out)	403
mDNS (UDP-Out)	404
mDNS (UDP-Out)	405
Microsoft Media Foundation Network Source OUT [TCP ALL]	406
Narrator	407
Narrator	408
Network Discovery (LLMNR-UDP-Out)	409
Network Discovery (NB-Datagram-Out)	410
Network Discovery (NB-Name-Out)	411
Network Discovery (Pub WSD-Out)	412
Network Discovery (SSDP-Out)	413
Network Discovery (UPnPHost-Out)	414
Network Discovery (UPnP-Out)	415
Network Discovery (WSD Events-Out)	416
Network Discovery (WSD EventsSecure-Out)	417
Network Discovery (WSD-Out)	418

Start	419
Start	420
Windows Default Lock Screen	421
Windows Default Lock Screen	422
Windows Defender SmartScreen	423
Windows Defender SmartScreen	424
Windows Device Management Certificate Installer (TCP out)	425
Windows Device Management Device Enroller (TCP out)	426
Windows Device Management Enrolment Service (TCP out)	427
Windows Device Management Sync Client (TCP out)	428
Windows Feature Experience Pack	429
Windows Feature Experience Pack	430
Windows Search	431
Windows Search	432
Windows Security	433
Windows Security	434
Windows Shell Experience	435
Windows Shell Experience	436
Windows Shell Experience	437
Windows Shell Experience	438
Workplace or school account	439
Workplace or school account	440
Your account	441
Your account	442
Windows Patches	443
Windows Update Configuration	444
Windows Update History	445
Software	446
.NET Framework	447

Documented Files	448
Machine Config (.NET 4)	449
Event Logs	456
Application	457
Forwarded Events	461
Hardware Events	463
Internet Explorer	465
Key Management Service	467
Security	469
Setup	476
System	480
Windows PowerShell	484
Environment Variables	493
Installed Software	495
Internet Settings	496
ODBC Configuration	497
ODBC Drivers	498
Data Sources	499
SQL Server Data Source	500
Operating System	501
PowerShell Settings	503
Processes	504
Registry	510
XIA Configuration Server Setup	511
XIA Configuration Server Database Name	513
Server Roles and Features	514
Startup Commands	521
Task Scheduler Library	522
GoogleUpdateTaskMachineCore{722D3B95-1358-4B6A-B6EA-1BA14905F9D7}	523

GoogleUpdateTaskMachineUA{B5FB06C2-DBE0-4D16-A4FB-4073AED798C6}	525
MicrosoftEdgeUpdateTaskMachineCore	527
MicrosoftEdgeUpdateTaskMachineUA	529
Process Explorer-TEST2022-sysadmin	531
Process Explorer-WIN-K885JAOFNON-Administrator	533
Windows Remote Management (WinRM)	535
Windows Services	537
Windows Services [A - I]	546
Windows Services [J - R]	623
Windows Services [S - Z]	679
Windows Time	772
Support Provisions	773
Network Support	774
Hardware Warranty	775
Version History	776

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

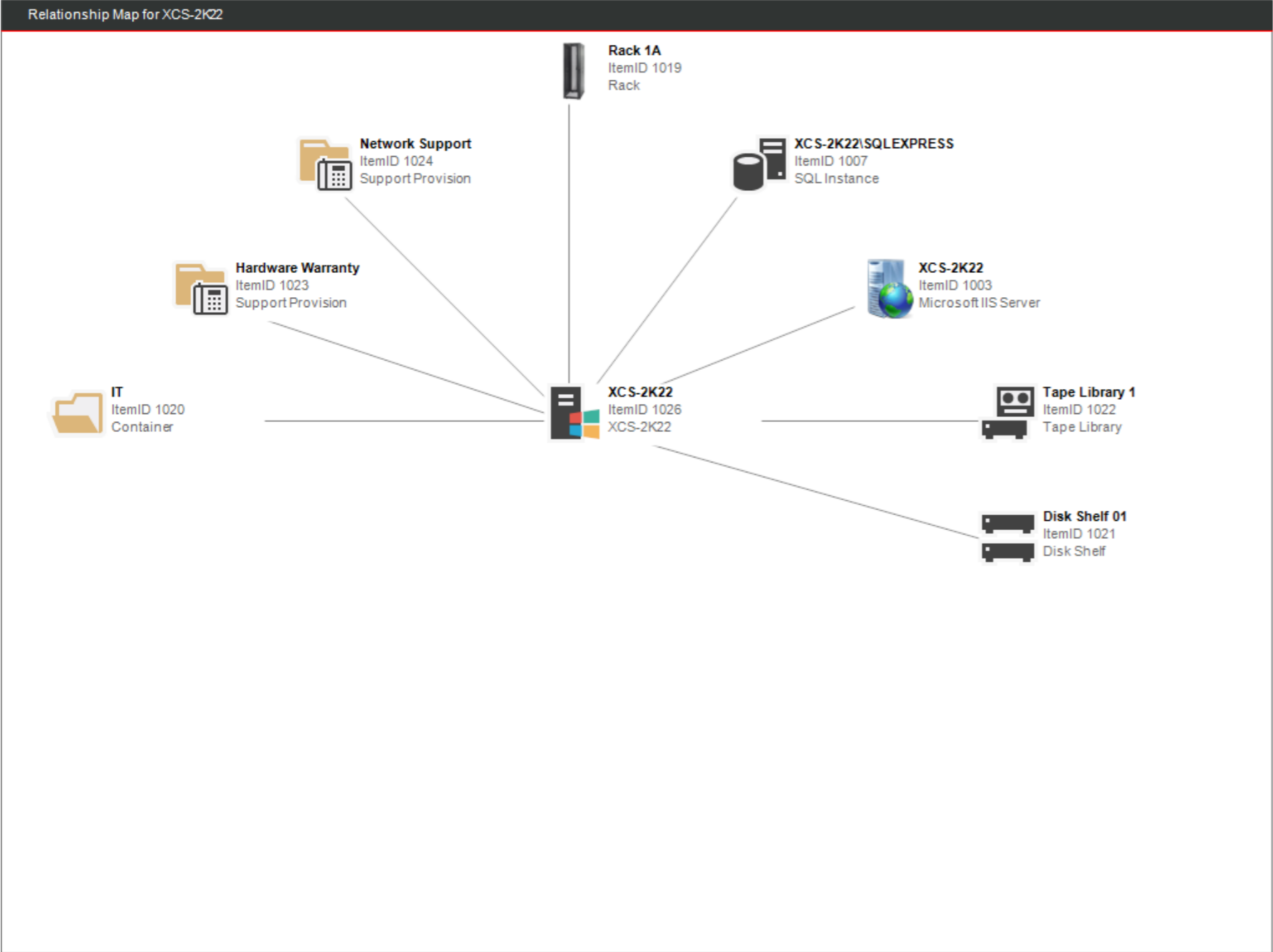
Relationships

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

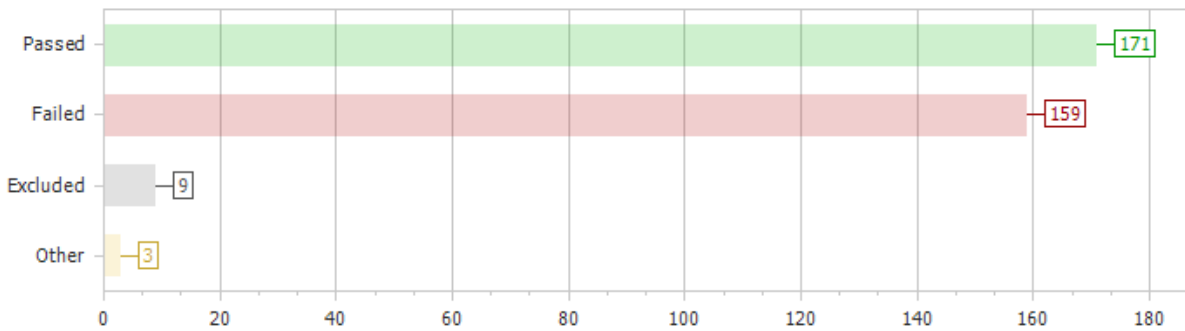
Compliance Benchmarks

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 apply to domain controllers)	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\adfsrv 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 <code>*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1</code> <code>*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1</code>	
📁 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:	NECVMMWar 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
--------------------	------------

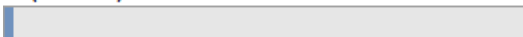
1 Partitions

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

C: (67% free)



Disk Shelves

Provides information about the disk shelves connected to this machine.

 1 Connected Disk Shelves

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

Disk Shelf 01

Disk Shelf 01


Item ID	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

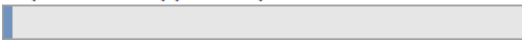
E: (ReFS Volume)

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

E: (ReFS Volume) (98% free)









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

Drive (70% free)



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.








System devices

Name	Driver Provider	Driver Version	Status
ACPI Fixed Feature Button	Microsoft	10.0.20348.1	Device is working properly.
Composite Bus Enumerator	Microsoft	10.0.20348.1	Device is working properly.
CPU to PCI Bridge	Microsoft	10.0.20348.1	Device is working properly.
Direct memory access controller	Microsoft	10.0.20348.1	Device is working properly.
EISA programmable interrupt controller	Microsoft	10.0.20348.1	Device is working properly.
Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
Generic Bus	Microsoft	10.0.20348.1	Device is working properly.

 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 Generic Bus	Microsoft	10.0.20348.1	Device is working properly.
 High Definition Audio Controller	Microsoft	10.0.20348.1	Device is working properly.
 High precision event timer	Microsoft	10.0.20348.1	Device is working properly.
 Microsoft ACPI-Compliant System	Microsoft	10.0.20348.1	Device is working properly.
 Microsoft Basic Display Driver	Microsoft	10.0.20348.1	Device is working properly.
 Microsoft Basic Render Driver	Microsoft	10.0.20348.1	Device is working properly.
 Microsoft Hyper-V Generation Counter	Microsoft	10.0.20348.1	Device is working properly.
 Microsoft System Management BIOS Driver	Microsoft	10.0.20348.1	Device is working properly.
 Microsoft Virtual Drive Enumerator	Microsoft	10.0.20348.1	Device is working properly.
 Motherboard resources	Microsoft	10.0.20348.1	Device is working properly.

 Remote Desktop Device Redirector Bus	Microsoft	10.0.20348.1	Device is working properly.
 System CMOS/real time clock	Microsoft	10.0.20348.1	Device is working properly.
 System speaker	Microsoft	10.0.20348.1	Device is working properly.
 System timer	Microsoft	10.0.20348.1	Device is working properly.
 UMBus Root Bus Enumerator	Microsoft	10.0.20348.1	Device is working properly.
 VMware VMCI Bus Device	VMware, Inc.	9.8.16.0	Device is working properly.
 VMware VMCI Host Device	VMware, Inc.	9.8.16.0	Device is working properly.
 Volume Manager	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.

Batteries

Microsoft AC Adapter

Microsoft AC Adapter

Class	Batteries
Class GUID	{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
Device Status	Device is working properly.
PNP Device Identifier	ACPIACPI0003\1
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	BATTERY
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	cmbatt.inf

Computer

ACPI x64-based PC

ACPI x64-based PC

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	COMPUTER
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	hal.inf

Disk drives

VMware Virtual NVMe Disk

VMware Virtual NVMe Disk

Class	Disk drives
Class GUID	{4d36e967-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	SCSI\DISK&VEN_NVME&PROD_VMWARE_VIRTUAL_N5&290F3806&0&000000
Manufacturer	(Standard disk drives)
Location	Bus Number 0, Target Id 0, LUN 0

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	DISKDRIVE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	VMware Virtual NVMe Disk
Inf Name	disk.inf

VMware Virtual SATA Hard Drive

VMware Virtual SATA Hard Drive

Class	Disk drives
Class GUID	{4d36e967-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	SCSI\DISK&VEN_VMWARE&PROD_VIRTUAL_SATA_HAR\5&3F6B946&0&000000
Manufacturer	(Standard disk drives)
Location	Bus Number 0, Target Id 0, LUN 0

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	DISKDRIVE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	VMware Virtual SATA Hard Drive
Inf Name	disk.inf

Display adapters

VMware SVGA 3D

VMware SVGA 3D

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

Driver Details

Driver Date	07 June 2021 01:00:00
Device Class	DISPLAY
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	8.17.3.5
Inf Name	oem8.inf

DVD/CD-ROM drives

NECVMMWar VMware SATA CD01

NECVMMWar VMware SATA CD01

Class	DVD/CD-ROM drives
Class GUID	{4d36e965-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	SCSI\CDROM&VEN_NECVMMWAR&PROD_VMWARE_SATA_CD01\5&3F6B946&0&010000
Manufacturer	(Standard CD-ROM drives)
Location	Bus Number 1, Target Id 0, LUN 0

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	CDROM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	NECVMMWar VMware SATA CD01
Inf Name	cdrom.inf

Human Interface Devices

USB Input Device

USB Input Device

Class	Human Interface Devices
Class GUID	{745a17a0-74d3-11d0-b6fe-00a0c90f57da}
Device Status	Device is working properly.
PNP Device Identifier	USB\VID_0E0F&PID_0003&MI_00\7&2DA3D997&0&0000
Manufacturer	(Standard system devices)
Location	000b.0000.0000.005.000.000.000.000

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	HIDCLASS
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	input.inf

USB Input Device

USB Input Device

Class	Human Interface Devices
Class GUID	{745a17a0-74d3-11d0-b6fe-00a0c90f57da}
Device Status	Device is working properly.
PNP Device Identifier	USB\VID_0E0F&PID_0003&MI_01\7&2DA3D997&0&0001
Manufacturer	(Standard system devices)
Location	000b.0000.0000.005.000.000.000.000

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	HIDCLASS
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	input.inf

IDE ATA/ATAPI controllers

ATA Channel 0

ATA Channel 0

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	HDC
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	ATA Channel 0
Inf Name	mshdc.inf

ATA Channel 1

ATA Channel 1

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	HDC
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	ATA Channel 1
Inf Name	mshdc.inf

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

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

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	HDC
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	mshdc.inf

Standard SATA AHCI Controller

Standard SATA AHCI Controller

Class	IDE ATA/ATAPI controllers
Class GUID	{4d36e96a-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_07E0&SUBSYS_07E015AD&REV_00\4&B70F118&0&2088
Manufacturer	Standard SATA AHCI Controller
Location	PCI bus 2, device 4, function 0

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	HDC
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	mshdc.inf

Keyboards

Standard PS/2 Keyboard

Standard PS/2 Keyboard

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	KEYBOARD
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	keyboard.inf

Mice and other pointing devices

VMware Pointing Device

VMware Pointing Device

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

Driver Details

Driver Date	07 November 2019
Device Class	MOUSE
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	12.5.10.0
Inf Name	oem7.inf

VMware USB Pointing Device

VMware USB Pointing Device

Class	Mice and other pointing devices
Class GUID	{4d36e96f-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	HID\VID_0E0F&PID_0003&MI_00\8&33601B94&0&0000
Manufacturer	VMware, Inc.

Driver Details

Driver Date	07 November 2019
Device Class	MOUSE
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	12.5.10.0
Inf Name	oem6.inf

VMware USB Pointing Device

VMware USB Pointing Device

Class	Mice and other pointing devices
Class GUID	{4d36e96f-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	HID\VID_0E0F&PID_0003&MI_01\8&3193129C&0&0000
Manufacturer	VMware, Inc.

Driver Details

Driver Date	07 November 2019
Device Class	MOUSE
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	12.5.10.0
Inf Name	oem6.inf

Monitors

Generic Non-PnP Monitor

Generic Non-PnP Monitor

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	MONITOR
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	monitor.inf

Network adapters

Intel(R) 82574L Gigabit Network Connection

Intel(R) 82574L Gigabit Network Connection

Class	Network adapters
Class GUID	{4d36e972-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_8086&DEV_10D3&SUBSYS_07D015AD&REV_00\000C29FFFFBD06DD00
Manufacturer	Intel Corporation
Location	PCI bus 3, device 0, function 0

Driver Details

Driver Date	06 October 2020 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	12.18.9.23
Friendly Name	Intel(R) 82574L Gigabit Network Connection
Inf Name	net1ix64.inf

Microsoft Kernel Debug Network Adapter

Microsoft Kernel Debug Network Adapter

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Microsoft Kernel Debug Network Adapter
Inf Name	kdnic.inf

WAN Miniport (GRE)

WAN Miniport (GRE)

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (GRE)
Inf Name	netgrea.inf

WAN Miniport (IKEv2)

WAN Miniport (IKEv2)

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (IKEv2)
Inf Name	netavpna.inf

WAN Miniport (IP)

WAN Miniport (IP)

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (IP)
Inf Name	netrasa.inf

WAN Miniport (IPv6)

WAN Miniport (IPv6)

Class	Network adapters
Class GUID	{4d36e972-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	SWD\MSRRAS\MS_NDISWANIPV6
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (IPv6)
Inf Name	netrasa.inf

WAN Miniport (L2TP)

WAN Miniport (L2TP)

Class	Network adapters
Class GUID	{4d36e972-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	SWD\MSRRAS\MS_L2TPMINIPOINT
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (L2TP)
Inf Name	netrasa.inf

WAN Miniport (Network Monitor)

WAN Miniport (Network Monitor)

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (Network Monitor)
Inf Name	netrasa.inf

WAN Miniport (PPPOE)

WAN Miniport (PPPOE)

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (PPPOE)
Inf Name	netrasa.inf

WAN Miniport (PPTP)

WAN Miniport (PPTP)

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (PPTP)
Inf Name	netrasa.inf

WAN Miniport (SSTP)

WAN Miniport (SSTP)

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	NET
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	WAN Miniport (SSTP)
Inf Name	netsstpa.inf

Ports (COM & LPT)

Communications Port (COM1)

Communications Port (COM1)

Class	Ports (COM & LPT)
Class GUID	{4d36e978-e325-11ce-bfc1-08002be10318}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\PNP0501\1
Manufacturer	(Standard port types)

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	PORTS
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Communications Port (COM1)
Inf Name	msports.inf

Print queues

Microsoft Print to PDF

Microsoft Print to PDF

Class	Print queues
Class GUID	{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}
Device Status	Device is working properly.
PNP Device Identifier	SWD\PRINTENUM\{43157E9F-CE2F-4107-8879-A4A553E5E904}
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	PRINTQUEUE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Microsoft Print to PDF
Inf Name	printqueue.inf

Microsoft XPS Document Writer

Microsoft XPS Document Writer

Class	Print queues
Class GUID	{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}
Device Status	Device is working properly.
PNP Device Identifier	SWD\PRINTENUM\{A6DC077D-DE36-46C9-A5B0-6C5F5BE521BC}
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	PRINTQUEUE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Microsoft XPS Document Writer
Inf Name	printqueue.inf

Root Print Queue

Root Print Queue


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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	PRINTQUEUE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Root Print Queue
Inf Name	printqueue.inf

Processors

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


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

Class	Processors
Class GUID	{50127dc3-0f36-415e-a6cc-4cb3be910b65}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\GENUINEINTEL_-INTEL64_FAMILY_6_MODEL_165_-INTEL(R)_CORE(TM)_I9-10885H_CPU_@_2.40GHZ\0
Manufacturer	Intel

 Driver Details

Driver Date	21 April 2009 01:00:00
Device Class	PROCESSOR
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz
Inf Name	cpu.inf

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

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

Class	Processors
Class GUID	{50127dc3-0f36-415e-a6cc-4cb3be910b65}
Device Status	Device is working properly.
PNP Device Identifier	ACPI\GENUINEINTEL_-INTEL64_FAMILY_6_MODEL_165_-INTEL(R)_CORE(TM)_I9-10885H_CPU_@_2.40GHZ\1
Manufacturer	Intel

 Driver Details

Driver Date	21 April 2009 01:00:00
Device Class	PROCESSOR
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz
Inf Name	cpu.inf

Software devices

Microsoft Radio Device Enumeration Bus

Microsoft Radio Device Enumeration Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SOFTWAREDEVICE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Microsoft Radio Device Enumeration Bus
Inf Name	c_swdevice.inf

Microsoft RRAS Root Enumerator

Microsoft RRAS Root Enumerator

Class	Software devices
Class GUID	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}
Device Status	Device is working properly.
PNP Device Identifier	SWD\MSRRAS\{5E259276-BC7E-40E3-B93B-8F89B5F3ABC0}
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SOFTWAREDEVICE
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Microsoft RRAS Root Enumerator
Inf Name	c_swdevice.inf

Sound, video and game controllers

High Definition Audio Device

High Definition Audio Device

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

Driver Details

Driver Date	05 July 2021 01:00:00
Device Class	MEDIA
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	hdaudio.inf

Storage controllers

Microsoft Storage Spaces Controller

Microsoft Storage Spaces Controller

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SCSIADAPTER
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.202
Inf Name	spaceport.inf

Standard NVM Express Controller

Standard NVM Express Controller

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SCSIADAPTER
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.202
Inf Name	stornvme.inf

Storage volumes

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{7AD56E60-0A72-11EC-BCFA-806E6F6E6963}#0000000EDF300000
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	volume.inf

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{C94278E7-2933-11ED-BD0D-000C29BD06DD}#0000000000100000
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	volume.inf

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{7AD56E60-0A72-11EC-BCFA-806E6F6E6963}#000000000100000
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	volume.inf

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{7AD56E60-0A72-11EC-BCFA-806E6F6E6963}#0000000007500000
Manufacturer	Microsoft

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	volume.inf

Volume

Volume

Class	Storage volumes
Class GUID	{71a27cdd-812a-11d0-bec7-08002be2092f}
Device Status	Device is working properly.
PNP Device Identifier	STORAGE\VOLUME\{7AD56E60-0A72-11EC-BCFA-806E6F6E6963}#0000000006500000
Manufacturer	Microsoft

 Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	VOLUME
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	volume.inf

System devices

ACPI Fixed Feature Button

ACPI Fixed Feature Button

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Composite Bus Enumerator

Composite Bus Enumerator

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	compositebus.inf

CPU to PCI Bridge

CPU to PCI Bridge

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Direct memory access controller

Direct memory access controller

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

EISA programmable interrupt controller

EISA programmable interrupt controller

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Generic Bus

Generic Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

High Definition Audio Controller

High Definition Audio Controller

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

Driver Details

Driver Date	05 July 2021 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	hdaudbus.inf

High precision event timer

High precision event timer

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Microsoft ACPI-Compliant System

Microsoft ACPI-Compliant System

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	acpi.inf

Microsoft Basic Display Driver

Microsoft Basic Display Driver

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	basicdisplay.inf

Microsoft Basic Render Driver

Microsoft Basic Render Driver

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	basicrender.inf

Microsoft Hyper-V Generation Counter

Microsoft Hyper-V Generation Counter

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	wgencounter.inf

Microsoft System Management BIOS Driver

Microsoft System Management BIOS Driver

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	mssmbios.inf

Microsoft Virtual Drive Enumerator

Microsoft Virtual Drive Enumerator

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	vdrvroot.inf

Motherboard resources

Motherboard resources

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

Motherboard resources

Motherboard resources

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

NDIS Virtual Network Adapter Enumerator

NDIS Virtual Network Adapter Enumerator

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	ndisvirtualbus.inf

PCI Bus

PCI Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI Express Root Port

PCI Express Root Port

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI to ISA Bridge

PCI to ISA Bridge

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

PCI-to-PCI Bridge

PCI-to-PCI Bridge

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

PCI-to-PCI Bridge

PCI-to-PCI Bridge

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	pci.inf

Plug and Play Software Device Enumerator

Plug and Play Software Device Enumerator

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

Driver Details

Driver Date	05 July 2021 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	swenum.inf

Remote Desktop Device Redirector Bus

Remote Desktop Device Redirector Bus

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	rdpbus.inf

System CMOS/real time clock

System CMOS/real time clock

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

System speaker

System speaker

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

System timer

System timer

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	machine.inf

UMBus Root Bus Enumerator

UMBus Root Bus Enumerator

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	umbus.inf

VMware VMCI Bus Device

VMware VMCI Bus Device

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

Driver Details

Driver Date	07 November 2019
Device Class	SYSTEM
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	9.8.16.0
Inf Name	oem2.inf

VMware VMCI Host Device

VMware VMCI Host Device

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

Driver Details

Driver Date	07 November 2019
Device Class	SYSTEM
Driver Provider	VMware, Inc.
Signed By	Microsoft Windows Hardware Compatibility Publisher
Driver Version	9.8.16.0
Inf Name	oem2.inf

Volume Manager

Volume Manager

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	SYSTEM
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	volmgr.inf

Universal Serial Bus controllers

Standard Enhanced PCI to USB Host Controller

Standard Enhanced PCI to USB Host Controller

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	usbport.inf

Standard Universal PCI to USB Host Controller

Standard Universal PCI to USB Host Controller

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	usbport.inf

Standard USB 3.1 eXtensible Host Controller - 1.0 (Microsoft)

Standard USB 3.1 eXtensible Host Controller - 1.0 (Microsoft)

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	PCI\VEN_15AD&DEV_0779&SUBSYS_077915AD&REV_00\4&AA0A8D5&0&00B0
Manufacturer	Generic USB xHCI Host Controller
Location	PCI bus 11, device 0, function 0

Driver Details

Driver Date	05 July 2021 01:00:00
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Friendly Name	Standard USB 3.1 eXtensible Host Controller - 1.0 (Microsoft)
Inf Name	usbxhci.inf

USB Composite Device

USB Composite Device

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	USB\VID_0E0F&PID_0003\6&38EEE119&0&5
Manufacturer	(Standard USB Host Controller)
Location	Port_#0005.Hub_#0003

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	usb.inf

USB Root Hub

USB Root Hub

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

Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	usbport.inf

USB Root Hub

USB Root Hub

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


Driver Details

Driver Date	21 June 2006 01:00:00
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	usbport.inf

USB Root Hub (USB 3.0)

USB Root Hub (USB 3.0)

Class	Universal Serial Bus controllers
Class GUID	{36fc9e60-c465-11cf-8056-444553540000}
Device Status	Device is working properly.
PNP Device Identifier	USB\ROOT_HUB30\5&31FDDB6C&0&0
Manufacturer	(Standard USB HUBs)

 Driver Details

Driver Date	05 July 2021 01:00:00
Device Class	USB
Driver Provider	Microsoft
Signed By	Microsoft Windows
Driver Version	10.0.20348.1
Inf Name	usbhub3.inf









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

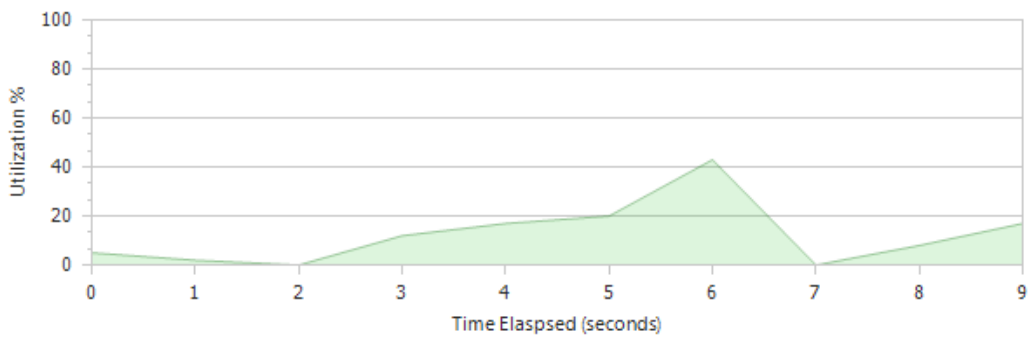
Processors

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	0F8BFBF000A0652
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.

14 Network Adapters

Name	Status	Device Name	MAC address
 6to4 Adapter	Device is working properly.		
 Ethernet (Kernel Debugger)	Device is working properly.	Microsoft Kernel Debug Network Adapter	
 Ethernet0	Device is working properly.	Intel(R) 82574L Gigabit Network Connection	00-0C-29-BD-06-DD
 Local Area Connection* 1	Not connected	WAN Miniport (SSTP)	
 Local Area Connection* 2	Not connected	WAN Miniport (IKEv2)	
 Local Area Connection* 3	Not connected	WAN Miniport (L2TP)	
 Local Area Connection* 4	Not connected	WAN Miniport (PPTP)	
 Local Area Connection* 5	Not connected	WAN Miniport (PPPOE)	
 Local Area Connection* 6	Not connected	WAN Miniport (GRE)	
 Local Area Connection* 7	Device is working properly.	WAN Miniport (IP)	
 Local Area Connection* 8	Device is working properly.	WAN Miniport (IPv6)	
 Local Area Connection* 9	Device is working properly.	WAN Miniport (Network Monitor)	
 Microsoft IP-HTTPS Platform Interface	Device is working properly.		
 Teredo Tunneling Pseudo-Interface	Device is working properly.		

6to4 Adapter

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

6to4 Adapter

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

Ethernet (Kernel Debugger)

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

Ethernet (Kernel Debugger)	
Index	0009
Device Name	Microsoft Kernel Debug Network Adapter
MAC Address	
Status	Device is working properly.
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{814CCED4-68C3-4B41-9DDD-9CB6CA7F160D}
Speed / Duplex	0 bps










Ethernet0

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

Ethernet0

Index	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

Local Area Connection* 1

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

Local Area Connection* 1	
Index	0008
Device Name	WAN Miniport (SSTP)
MAC Address	
Status	Not connected
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{77E737F6-FA5B-48E2-8C67-68C539A61825}
Speed / Duplex	0 bps

Local Area Connection* 2

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

Local Area Connection* 2	
Index	0014
Device Name	WAN Miniport (IKEv2)
MAC Address	
Status	Not connected
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{C29B7316-7856-4885-9243-1A2762C67C76}
Speed / Duplex	0 bps

Local Area Connection* 3

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

Local Area Connection* 3	
Index	0015
Device Name	WAN Miniport (L2TP)
MAC Address	
Status	Not connected
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{E15C69E2-8D95-4B87-8B3D-87925692F8CB}
Speed / Duplex	0 bps

Local Area Connection* 4

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

Local Area Connection* 4	
Index	0004
Device Name	WAN Miniport (PPTP)
MAC Address	
Status	Not connected
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{1B60866F-E90F-469B-9EE5-FB31A29DD244}
Speed / Duplex	0 bps

Local Area Connection* 5

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

Local Area Connection* 5	
Index	0003
Device Name	WAN Miniport (PPPOE)
MAC Address	
Status	Not connected
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{15FB3946-F220-4FDE-912E-FE5645DB9362}
Speed / Duplex	0 bps

Local Area Connection* 6

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

Local Area Connection* 6	
Index	0006
Device Name	WAN Miniport (GRE)
MAC Address	
Status	Not connected
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{45377327-D169-4FB6-AF7F-2FB1CA32974D}
Speed / Duplex	0 bps

Local Area Connection* 7

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

Local Area Connection* 7	
Index	0013
Device Name	WAN Miniport (IP)
MAC Address	
Status	Device is working properly.
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{BC465C6F-A2C4-49DB-AC0C-15D4A5ABADD9}
Speed / Duplex	0 bps

Local Area Connection* 8

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

Local Area Connection* 8	
Index	0007
Device Name	WAN Miniport (IPv6)
MAC Address	
Status	Device is working properly.
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{5407BAD7-8582-4C0B-8E33-51EAC80F2A7A}
Speed / Duplex	0 bps

Local Area Connection* 9

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

Local Area Connection* 9	
Index	0010
Device Name	WAN Miniport (Network Monitor)
MAC Address	
Status	Device is working properly.
Driver Date	2006-06-21
Driver Version	10.0.20348.1
Physical Adapter	False
Interface GUID	{8BDB378F-CE4F-4EB6-BFE4-BFCDAB61412D}
Speed / Duplex	0 bps

Microsoft IP-HTTPS Platform Interface

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

Microsoft IP-HTTPS Platform Interface

Index	0005
Device Name	
MAC Address	
Status	Device is working properly.
Driver Date	
Driver Version	
Physical Adapter	False
Interface GUID	{2EE2C70C-A092-4D88-A654-98C8D7645CD5}
Speed / Duplex	0 bps

Teredo Tunneling Pseudo-Interface

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

Teredo Tunneling Pseudo-Interface	
Index	0011
Device Name	
MAC Address	
Status	Device is working properly.
Driver Date	
Driver Version	
Physical Adapter	False
Interface GUID	{93123211-9629-4E04-82F0-EA2E4F221468}
Speed / Duplex	0 bps

Network Load Balancing

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

General Settings












Enabled

False

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\$

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\$

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

Intermediate Certification Authorities

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

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

 3 Certificates

Subject	Issuer	Expiry Date
 Microsoft Windows Hardware Compatibility	Microsoft Root Authority	31 December 2002
 Root Agency	Root Agency	31 December 2039
 www.verisign.com/CPS Incorporation by Reference. LIABILITY LIMITED BY OUR TERMS OF SERVICE. (c) 1997 VeriSign	Class 3 Public Primary Certification Authority	24 October 2016

Microsoft Windows Hardware Compatibility

Provides details of the X.509 certificate.

General

Subject Name	Microsoft Windows Hardware Compatibility
Subject	CN=Microsoft Windows Hardware Compatibility, OU=Microsoft Corporation, OU=Microsoft Windows Hardware Compatibility Intermediate CA, OU=Copyright (c) 1997 Microsoft Corp.
Issuer	CN=Microsoft Root Authority, OU=Microsoft Corporation, OU=Copyright (c) 1997 Microsoft Corp.
Issuer Name	Microsoft Root Authority
Valid From	01 October 1997
Expiry Date	31 December 2002
Key Usage	
Enhanced Key Usages	Code Signing (1.3.6.1.5.5.7.3.3) Windows Hardware Driver Verification (1.3.6.1.4.1.311.10.3.5)

Certificate Details

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

Properties

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

Root Agency

Provides details of the X.509 certificate.

General

Subject Name	Root Agency
Subject	CN=Root Agency
Issuer	CN=Root Agency
Issuer Name	Root Agency
Valid From	28 May 1996
Expiry Date	31 December 2039
Key Usage	
Enhanced Key Usages	

Certificate Details

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

Properties

Friendly Name	
Thumbprint	FEE449EE0E3965A5246F000E87FDE2A065FD89D4
Purposes	Enable all purposes for this certificate

Provides details of the X.509 certificate.

 General

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

 Certificate Details

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


 Properties

Friendly Name	
Thumbprint	D559A586669B08F46A30A133F8A9ED3D038E2EA8
Purposes	Enable all purposes for this certificate

Personal

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

 1 Certificates

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

Third-Party Root Certification Authorities

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

16 Certificates

Subject	Issuer	Expiry Date
 AAA Certificate Services	AAA Certificate Services	31 December 2028
 Baltimore CyberTrust Root	Baltimore CyberTrust Root	12 May 2025
 Class 3 Public Primary Certification Authority	Class 3 Public Primary Certification Authority	01 August 2028
 DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10 November 2031
 DigiCert Global Root CA	DigiCert Global Root CA	10 November 2031
 DigiCert Global Root G2	DigiCert Global Root G2	15 January 2038
 DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	10 November 2031
 DigiCert Trusted Root G4	DigiCert Trusted Root G4	15 January 2038
 DST Root CA X3	DST Root CA X3	30 September 2021
 Entrust Root Certification Authority - G2	Entrust Root Certification Authority - G2	07 December 2030
 GlobalSign	GlobalSign	18 March 2029
 GlobalSign Root CA	GlobalSign Root CA	28 January 2028
 Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Authority	29 June 2034
 QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	12 January 2042
 Starfield Class 2 Certification Authority	Starfield Class 2 Certification Authority	29 June 2034
 VeriSign Class 3 Public Primary Certification Authority - G5	VeriSign Class 3 Public Primary Certification Authority - G5	16 July 2036

AAA Certificate Services

Provides details of the X.509 certificate.

General

Subject Name	AAA Certificate Services
Subject	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, S=Greater Manchester, C=GB
Issuer	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, S=Greater Manchester, C=GB
Issuer Name	AAA Certificate Services
Valid From	01 January 2004
Expiry Date	31 December 2028
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	01
Signature Algorithm	sha1RSA
Version	3
CRL Distribution Points	http://crl.comodoca.com/AAACertificateServices.crl http://crl.comodo.net/AAACertificateServices.crl
Subject Alternative Names	

Properties

Friendly Name	Sectigo (AAA)
Thumbprint	D1EB23A46D17D68FD92564C2F1F1601764D8E349
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Encrypting File System (1.3.6.1.4.1.311.10.3.4) Secure Email (1.3.6.1.5.5.7.3.4) IP security tunnel termination (1.3.6.1.5.5.7.3.6) IP security user (1.3.6.1.5.5.7.3.7) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

Baltimore CyberTrust Root

Provides details of the X.509 certificate.

General

Subject Name	Baltimore CyberTrust Root
Subject	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
Issuer	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
Issuer Name	Baltimore CyberTrust Root
Valid From	12 May 2000
Expiry Date	12 May 2025
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	020000B9
Signature Algorithm	sha1RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	DigiCert Baltimore Root
Thumbprint	D4DE20D05E66FC53FE1A50882C78DB2852CAE474
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) OCSP Signing (1.3.6.1.5.5.7.3.9) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

Class 3 Public Primary Certification Authority

Provides details of the X.509 certificate.

General

Subject Name	Class 3 Public Primary Certification Authority
Subject	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Issuer	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Issuer Name	Class 3 Public Primary Certification Authority
Valid From	29 January 1996
Expiry Date	01 August 2028
Key Usage	
Enhanced Key Usages	

Certificate Details

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

Properties

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

DigiCert Assured ID Root CA

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

DigiCert Global Root CA

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

DigiCert Global Root G2

Provides details of the X.509 certificate.

General

Subject Name	DigiCert Global Root G2
Subject	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer Name	DigiCert Global Root G2
Valid From	01 August 2013
Expiry Date	15 January 2038
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

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

Properties

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

DigiCert High Assurance EV Root CA

Provides details of the X.509 certificate.

General

Subject Name	DigiCert High Assurance EV Root CA
Subject	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer Name	DigiCert High Assurance EV Root CA
Valid From	10 November 2006
Expiry Date	10 November 2031
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	02AC5C266A0B409B8F0B79F2AE462577
Signature Algorithm	sha1RSA
Authority Key Identifier	b13ec36903f8bf4701d498261a0802ef63642bc3
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	DigiCert
Thumbprint	5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

DigiCert Trusted Root G4

Provides details of the X.509 certificate.

General

Subject Name	DigiCert Trusted Root G4
Subject	CN=DigiCert Trusted Root G4, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer	CN=DigiCert Trusted Root G4, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer Name	DigiCert Trusted Root G4
Valid From	01 August 2013
Expiry Date	15 January 2038
Key Usage	Certificate signing CRL signing Digital Signature
Enhanced Key Usages	

Certificate Details

Public Key	RSA (4096 Bits)
Serial Number	059B1B579E8E2132E23907BDA777755C
Signature Algorithm	sha384RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	DigiCert Trusted Root G4
Thumbprint	DDFB16CD4931C973A2037D3FC83A4D7D775D05E4
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

DST Root CA X3

Provides details of the X.509 certificate.

General

Subject Name	DST Root CA X3
Subject	CN=DST Root CA X3, O=Digital Signature Trust Co.
Issuer	CN=DST Root CA X3, O=Digital Signature Trust Co.
Issuer Name	DST Root CA X3
Valid From	30 September 2000
Expiry Date	30 September 2021
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	44AFB080D6A327BA893039862EF8406B
Signature Algorithm	sha1RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	DST Root CA X3
Thumbprint	DAC9024F54D8F6DF94935FB1732638CA6AD77C13
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Document Signing (1.3.6.1.4.1.311.10.3.12) Encrypting File System (1.3.6.1.4.1.311.10.3.4) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

Entrust Root Certification Authority - G2

Provides details of the X.509 certificate.

General

Subject Name	Entrust Root Certification Authority - G2
Subject	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
Issuer	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
Issuer Name	Entrust Root Certification Authority - G2
Valid From	07 July 2009
Expiry Date	07 December 2030
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	4A538C28
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Entrust.net
Thumbprint	8CF427FD790C3AD166068DE81E57EFBB932272D4
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Encrypting File System (1.3.6.1.4.1.311.10.3.4) Secure Email (1.3.6.1.5.5.7.3.4) IP security tunnel termination (1.3.6.1.5.5.7.3.6) IP security user (1.3.6.1.5.5.7.3.7) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

Provides details of the X.509 certificate.

General

Subject Name	GlobalSign
Subject	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3
Issuer	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3
Issuer Name	GlobalSign
Valid From	18 March 2009
Expiry Date	18 March 2029
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	04000000000121585308A2
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	GlobalSign Root CA - R3
Thumbprint	D69B561148F01C77C54578C10926DF5B856976AD
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Encrypting File System (1.3.6.1.4.1.311.10.3.4) Secure Email (1.3.6.1.5.5.7.3.4) IP security tunnel termination (1.3.6.1.5.5.7.3.6) IP security user (1.3.6.1.5.5.7.3.7) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

GlobalSign Root CA

Provides details of the X.509 certificate.

General

Subject Name	GlobalSign Root CA
Subject	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Issuer	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Issuer Name	GlobalSign Root CA
Valid From	01 September 1998
Expiry Date	28 January 2028
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

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

Properties

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

Go Daddy Class 2 Certification Authority

Provides details of the X.509 certificate.

General

Subject Name	Go Daddy Class 2 Certification Authority
Subject	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US
Issuer	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US
Issuer Name	Go Daddy Class 2 Certification Authority
Valid From	29 June 2004
Expiry Date	29 June 2034
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	00
Signature Algorithm	sha1RSA
Authority Key Identifier	d2c4b0d291d44c1171b361cb3da1fedda86ad4e3
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Go Daddy Class 2 Certification Authority
Thumbprint	2796BAE63F1801E277261BA0D77770028F20EEE4
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1)

QuoVadis Root CA 2 G3

Provides details of the X.509 certificate.

General

Subject Name	QuoVadis Root CA 2 G3
Subject	CN=QuoVadis Root CA 2 G3, O=QuoVadis Limited, C=BM
Issuer	CN=QuoVadis Root CA 2 G3, O=QuoVadis Limited, C=BM
Issuer Name	QuoVadis Root CA 2 G3
Valid From	12 January 2012
Expiry Date	12 January 2042
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (4096 Bits)
Serial Number	445734245B81899B35F2CEB82B3B5BA726F07528
Signature Algorithm	sha256RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	QuoVadis Root CA 2 G3
Thumbprint	093C61F38B8BDC7D55DF7538020500E125F5C836
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) OCSP Signing (1.3.6.1.5.5.7.3.9) Server Authentication (1.3.6.1.5.5.7.3.1) Time Stamping (1.3.6.1.5.5.7.3.8)

Starfield Class 2 Certification Authority

Provides details of the X.509 certificate.

General

Subject Name	Starfield Class 2 Certification Authority
Subject	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US
Issuer	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US
Issuer Name	Starfield Class 2 Certification Authority
Valid From	29 June 2004
Expiry Date	29 June 2034
Key Usage	
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	00
Signature Algorithm	sha1RSA
Authority Key Identifier	bf5fb7d1cedd1f86f45b55acdc710c20ea988e7
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	Starfield Class 2 Certification Authority
Thumbprint	AD7E1C28B064EF8F6003402014C3D0E3370EB58A
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1)

VeriSign Class 3 Public Primary Certification Authority - G5

Provides details of the X.509 certificate.

General

Subject Name	VeriSign Class 3 Public Primary Certification Authority - G5
Subject	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
Issuer	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Valid From	08 November 2006
Expiry Date	16 July 2036
Key Usage	Certificate signing CRL signing
Enhanced Key Usages	

Certificate Details

Public Key	RSA (2048 Bits)
Serial Number	18DAD19E267DE8BB4A2158CDCC6B3B4A
Signature Algorithm	sha1RSA
Version	3
CRL Distribution Points	
Subject Alternative Names	

Properties

Friendly Name	VeriSign
Thumbprint	4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
Purposes	Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1)

Trusted People

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

There are no certificates in this store.

Trusted Publisher


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

There are no certificates in this store.

Trusted Root Certification Authorities

Trusted Root Certification Authorities contains root certificates from your organisation and Microsoft. Please note, unlike the Microsoft Certificates MMC this does NOT also include the certificates from the Third-Party Root Certification Authorities.

 13 Certificates

Subject	Issuer	Expiry Date
 Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	30 December 1999
 Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	31 December 1999
 Microsoft ECC Product Root Certificate Authority 2018	Microsoft ECC Product Root Certificate Authority 2018	27 February 2043
 Microsoft ECC TS Root Certificate Authority 2018	Microsoft ECC TS Root Certificate Authority 2018	27 February 2043
 Microsoft Root Authority	Microsoft Root Authority	31 December 2020
 Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	09 May 2021
 Microsoft Root Certificate Authority 2010	Microsoft Root Certificate Authority 2010	23 June 2035
 Microsoft Root Certificate Authority 2011	Microsoft Root Certificate Authority 2011	22 March 2036
 Microsoft Time Stamp Root Certificate Authority 2014	Microsoft Time Stamp Root Certificate Authority 2014	22 October 2039
 NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	07 January 2004
 Symantec Enterprise Mobile Root for Microsoft	Symantec Enterprise Mobile Root for Microsoft	14 March 2032
 Thawte Timestamping CA	Thawte Timestamping CA	31 December 2020
 WMSvc-SHA2-XCS-2K22	WMSvc-SHA2-XCS-2K22	30 August 2031

Copyright (c) 1997 Microsoft Corp.

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

Microsoft Authenticode(tm) Root Authority

Provides details of the X.509 certificate.

General

Subject Name	Microsoft Authenticode(tm) Root Authority
Subject	CN=Microsoft Authenticode(tm) Root Authority, O=MSFT, C=US
Issuer	CN=Microsoft Authenticode(tm) Root Authority, O=MSFT, C=US
Issuer Name	Microsoft Authenticode(tm) Root Authority
Valid From	01 January 1995
Expiry Date	31 December 1999
Key Usage	
Enhanced Key Usages	

Certificate Details

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

Properties

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

Microsoft ECC Product Root Certificate Authority 2018

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

Microsoft ECC TS Root Certificate Authority 2018

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

Microsoft Root Authority

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

Microsoft Root Certificate Authority

Provides details of the X.509 certificate.

General

Subject Name	Microsoft Root Certificate Authority
Subject	CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com
Issuer	CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com
Issuer Name	Microsoft Root Certificate Authority
Valid From	09 May 2001
Expiry Date	09 May 2021
Key Usage	Certificate signing CRL signing Digital Signature Non-repudiation
Enhanced Key Usages	

Certificate Details

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

Properties

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

Microsoft Root Certificate Authority 2010

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

Microsoft Root Certificate Authority 2011

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

Microsoft Time Stamp Root Certificate Authority 2014

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

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

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

Provides details of the X.509 certificate.

General

Subject Name	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
Subject	OU="NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.", OU=VeriSign Time Stamping Service Root, OU="VeriSign, Inc.", O=VeriSign Trust Network
Issuer	OU="NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.", OU=VeriSign Time Stamping Service Root, OU="VeriSign, Inc.", O=VeriSign Trust Network
Issuer Name	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
Valid From	12 May 1997
Expiry Date	07 January 2004
Key Usage	
Enhanced Key Usages	

Certificate Details

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

Properties

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

Symantec Enterprise Mobile Root for Microsoft

Provides details of the X.509 certificate.

General

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

Certificate Details

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

Properties

Friendly Name	
Thumbprint	92B46C76E13054E104F230517E6E504D43AB10B5
Purposes	Code Signing (1.3.6.1.5.5.7.3.3)

Thawte Timestamping CA

Provides details of the X.509 certificate.

General

Subject Name	Thawte Timestamping CA
Subject	CN=Thawte Timestamping CA, OU=Thawte Certification, O=Thawte, L=Durbanville, S=Western Cape, C=ZA
Issuer	CN=Thawte Timestamping CA, OU=Thawte Certification, O=Thawte, L=Durbanville, S=Western Cape, C=ZA
Issuer Name	Thawte Timestamping CA
Valid From	01 January 1997
Expiry Date	31 December 2020
Key Usage	
Enhanced Key Usages	

Certificate Details

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

Properties

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

WMSvc-SHA2-XCS-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

** Dynamic TCP incoming

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	RPC
Remote Ports	Any

** TCP Port 1433

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	1433
Remote Ports	Any

** UDP Port 1434

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	1434
Remote Ports	Any

AllJoyn Router (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for AllJoyn Router traffic [TCP]
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	9955
Remote Ports	Any

AllJoyn Router (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for AllJoyn Router traffic [UDP]
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Cast to Device functionality (qWave-TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [TCP 2177]
Direction	Inbound
Enabled	True
Profile Names	Private, Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	TCP
Local Ports	2177
Remote Ports	Any

Cast to Device functionality (qWave-UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [UDP 2177]
Direction	Inbound
Enabled	True
Profile Names	Private, Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	UDP
Local Ports	2177
Remote Ports	Any

Cast to Device SSDP Discovery (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule to allow discovery of Cast to Device targets using SSDP
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	PlayToDiscovery
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for the Cast to Device server to allow streaming using HTTP. [TCP 10246]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	10246
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for the Cast to Device server to allow streaming using HTTP. [TCP 10246]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	TCP
Local Ports	10246
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for the Cast to Device server to allow streaming using HTTP. [TCP 10246]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	TCP
Local Ports	10246
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [TCP 23554, 23555, 23556]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	23554, 23555, 23556
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [TCP 23554, 23555, 23556]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	TCP
Local Ports	23554, 23555, 23556
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [TCP 23554, 23555, 23556]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	TCP
Local Ports	23554, 23555, 23556
Remote Ports	Any

Cast to Device UPnP Events (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule to allow receiving UPnP Events from Cast to Device targets
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	TCP
Local Ports	2869
Remote Ports	Any

Core Networking - Destination Unreachable (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Destination Unreachable error messages are sent from any node that a packet traverses which is unable to forward the packet for any reason except congestion.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Destination Unreachable Fragmentation Needed error messages are sent from any node that a packet traverses which is unable to forward the packet because fragmentation was needed and the don't fragment bit was set.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv4
Local Ports	RPC
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	68
Remote Ports	67

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Allows DHCPV6 (Dynamic Host Configuration Protocol for IPv6) messages for stateful and stateless configuration.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	546
Remote Ports	547

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	IGMP messages are sent and received by nodes to create, join and depart multicast groups.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	2
Local Ports	Any
Remote Ports	Any

Core Networking - IPHTTPS (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound TCP rule to allow IPHTTPS tunnelling technology to provide connectivity across HTTP proxies and firewalls.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	IPHTTPSIn
Remote Ports	Any

Core Networking - IPv6 (IPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunnelling services.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	41
Local Ports	Any
Remote Ports	Any

Core Networking - Multicast Listener Done (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Multicast Listener Done messages inform local routers that there are no longer any members remaining for a specific multicast address on the subnet.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Query (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	An IPv6 multicast-capable router uses the Multicast Listener Query message to query a link for multicast group membership.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Report (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Multicast Listener Report v2 message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Neighbour Discovery Advertisement (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Neighbour Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbour Discovery Solicitation request.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Neighbour Discovery Solicitation (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Neighbour Discovery Solicitations are sent by nodes to discover the link-layer address of another on-link IPv6 node.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Packet Too Big (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Packet Too Big error messages are sent from any node that a packet traverses which is unable to forward the packet because the packet is too large for the next link.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Parameter Problem (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Parameter Problem error messages are sent by nodes as a result of incorrectly generated packets.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Router Advertisement (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Router Advertisement messages are sent by routers to other nodes for stateless auto-configuration.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	fe80::/64

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Router Solicitation (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Router Solicitation messages are sent by nodes seeking routers to provide stateless auto-configuration.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Teredo (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound UDP rule to allow Teredo edge traversal, a technology that provides address assignment and automatic tunnelling for unicast IPv6 traffic when an IPv6/IPv4 host is located behind an IPv4 network address translator.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Teredo
Remote Ports	Any

Core Networking - Time Exceeded (ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Time Exceeded error messages are generated from any node that a packet traverses if the Hop Limit value is decremented to zero at any point on the path.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Delivery Optimization (TCP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule to allow Delivery Optimization to connect to remote endpoints
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	7680
Remote Ports	Any

Delivery Optimization (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule to allow Delivery Optimization to connect to remote endpoints
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	7680
Remote Ports	Any

Desktop App Web Viewer

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Desktop App Web Viewer
Direction	Inbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Desktop App Web Viewer

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Desktop App Web Viewer
Direction	Inbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

DIAL protocol server (HTTP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for DIAL protocol server to allow remote control of Apps using HTTP. [TCP 10247]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	TCP
Local Ports	10247
Remote Ports	Any

DIAL protocol server (HTTP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for DIAL protocol server to allow remote control of Apps using HTTP. [TCP 10247]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	10247
Remote Ports	Any

File and Printer Sharing (Echo Request - ICMPv4-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Echo Request messages are sent as ping requests to other nodes.
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv4
Local Ports	RPC
Remote Ports	Any

File and Printer Sharing (Echo Request - ICMPv6-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Echo Request messages are sent as ping requests to other nodes.
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

File and Printer Sharing (LLMNR-UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for File and Printer Sharing to allow Link Local Multicast Name Resolution. [UDP 5355]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	5355
Remote Ports	Any

File and Printer Sharing (NB-Datagram-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for File and Printer Sharing to allow NetBIOS Datagram transmission and reception. [UDP 138]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	138
Remote Ports	Any

File and Printer Sharing (NB-Name-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for File and Printer Sharing to allow NetBIOS Name Resolution. [UDP 137]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	137
Remote Ports	Any

File and Printer Sharing (NB-Session-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for File and Printer Sharing to allow NetBIOS Session Service connections. [TCP 139]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	139
Remote Ports	Any

File and Printer Sharing (SMB-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for File and Printer Sharing to allow Server Message Block transmission and reception via Named Pipes. [TCP 445]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	445
Remote Ports	Any

File and Printer Sharing (Spooler Service - RPC)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\spoolsv.exe
Description	Inbound rule for File and Printer Sharing to allow the Print Spooler Service to communicate via TCP/RPC.
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	RPC
Remote Ports	Any

File and Printer Sharing (Spooler Service - RPC-EPMAP)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for the RPCSS service to allow RPC/TCP traffic for the Spooler Service.
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	RPCSEMap
Remote Ports	Any

File Server Remote Management (DCOM-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule to allow DCOM traffic to manage the File Services role.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	135
Remote Ports	Any

File Server Remote Management (SMB-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule to allow SMB traffic to manage the File Services role.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	445
Remote Ports	Any

File Server Remote Management (WMI-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule to allow WMI traffic to manage the File Services role.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	RPC
Remote Ports	Any

Google Chrome (mDNS-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Program Files\Google\Chrome\Application\chrome.exe
Description	Inbound rule for Google Chrome to allow mDNS traffic.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

mDNS (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for mDNS traffic [UDP]
Direction	Inbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

mDNS (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for mDNS traffic [UDP]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

mDNS (UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for mDNS traffic [UDP]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

Microsoft Edge (mDNS-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
Description	Inbound rule for Microsoft Edge to allow mDNS traffic.
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	5353
Remote Ports	Any

Microsoft Media Foundation Network Source IN [TCP 554]

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	InBound Rule for the Microsoft Media Foundation's Capture SVC to open TCP port to enable RTSP
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	TCP
Local Ports	554, 8554-8558
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	InBound Rule for the Microsoft Media Foundation's Capture SVC to open UDP port to enable RTSP
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	5000-5020
Remote Ports	Any

Network Discovery (LLMNR-UDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for Network Discovery to allow Link Local Multicast Name Resolution. [UDP 5355]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	5355
Remote Ports	Any

Network Discovery (NB-Datagram-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for Network Discovery to allow NetBIOS Datagram transmission and reception. [UDP 138]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	138
Remote Ports	Any

Network Discovery (NB-Name-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for Network Discovery to allow NetBIOS Name Resolution. [UDP 137]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	137
Remote Ports	Any

Network Discovery (Pub-WSD-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for Network Discovery to discover devices via Function Discovery. [UDP 3702]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	3702
Remote Ports	Any

Network Discovery (SSDP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for Network Discovery to allow use of the Simple Service Discovery Protocol. [UDP 1900]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	1900
Remote Ports	Any

Network Discovery (UPnP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for Network Discovery to allow use of Universal Plug and Play. [TCP 2869]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	2869
Remote Ports	Any

Network Discovery (WSD Events-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for Network Discovery to allow WSDAPI Events via Function Discovery. [TCP 5357]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	5357
Remote Ports	Any

Network Discovery (WSD EventsSecure-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for Network Discovery to allow Secure WSDAPI Events via Function Discovery. [TCP 5358]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	5358
Remote Ports	Any

Network Discovery (WSD-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule for Network Discovery to discover devices via Function Discovery. [UDP 3702]
Direction	Inbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	3702
Remote Ports	Any

Start

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Start
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Start

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Start
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Web Management Service (HTTP Traffic-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	system
Description	An inbound rule to allow Web Management Service traffic for Internet Information Services (IIS) [TCP 8172]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	8172
Remote Ports	Any

Windows Management Instrumentation (DCOM-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule to allow DCOM traffic for remote Windows Management Instrumentation. [TCP 135]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	135
Remote Ports	Any

Windows Management Instrumentation (WMI-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Inbound rule to allow WMI traffic for remote Windows Management Instrumentation. [TCP]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Windows Remote Management (HTTP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for Windows Remote Management via WS-Management. [TCP 5985]
Direction	Inbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	TCP
Local Ports	5985
Remote Ports	Any

Windows Remote Management (HTTP-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Inbound rule for Windows Remote Management via WS-Management. [TCP 5985]
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	5985
Remote Ports	Any

Windows Search

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Search the web and Windows
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Search

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Search the web and Windows
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Workplace or school account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Workplace or school account
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Workplace or school account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Workplace or school account
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

World Wide Web Services (HTTP Traffic-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	An inbound rule to allow HTTP traffic for Internet Information Services (IIS) [TCP 80]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	80
Remote Ports	Any

World Wide Web Services (HTTPS Traffic-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	An inbound rule to allow HTTPS traffic for Internet Information Services (IIS) [TCP 443]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	443
Remote Ports	Any

World Wide Web Services (QUIC Traffic-In)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	An inbound rule to allow QUIC traffic for Internet Information Services (IIS) [UDP 443]
Direction	Inbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	443
Remote Ports	Any

Your account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Your account
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Your account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Your account
Direction	Inbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Outbound Rules

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

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
✔ 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

AllJoyn Router (TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for AllJoyn Router traffic [TCP]
Direction	Outbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

AllJoyn Router (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for AllJoyn Router traffic [UDP]
Direction	Outbound
Enabled	True
Profile Names	Domain, Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Captive Portal Flow

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Captive Portal Flow
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Captive Portal Flow

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Captive Portal Flow
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Cast to Device functionality (qWave-TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [TCP 2177]
Direction	Outbound
Enabled	True
Profile Names	Private, Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	2177

Cast to Device functionality (qWave-UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [UDP 2177]
Direction	Outbound
Enabled	True
Profile Names	Private, Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	2177

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Outbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Outbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Outbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	PlayToDevice

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\mdeserver.exe
Description	Outbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Connected User Experiences and Telemetry

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Unified Telemetry Client Outbound Traffic
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	443

Core Networking - DNS (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule to allow DNS requests. DNS responses based on requests that matched this rule will be permitted regardless of source address. This behaviour is classified as loose source mapping. [LSM] [UDP 53]
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	53

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	68
Remote Ports	67

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Allows DHCPV6 (Dynamic Host Configuration Protocol for IPv6) messages for stateful and stateless configuration.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	546
Remote Ports	547

Core Networking - Group Policy (LSASS-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\lsass.exe
Description	Outbound rule to allow remote LSASS traffic for Group Policy updates [TCP].
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Core Networking - Group Policy (NP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Core Networking - Group Policy (NP-Out)
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	445

Core Networking - Group Policy (TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule to allow remote RPC traffic for Group Policy updates. [TCP]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	IGMP messages are sent and received by nodes to create, join and depart multicast groups.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	2
Local Ports	Any
Remote Ports	Any

Core Networking - IPHTTPS (TCP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound TCP rule to allow IPHTTPS tunnelling technology to provide connectivity across HTTP proxies and firewalls.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	IPHTTPSOut

Core Networking - IPv6 (IPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunnelling services.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	41
Local Ports	Any
Remote Ports	Any

Core Networking - Multicast Listener Done (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Multicast Listener Done messages inform local routers that there are no longer any members remaining for a specific multicast address on the subnet.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Query (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	An IPv6 multicast-capable router uses the Multicast Listener Query message to query a link for multicast group membership.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Multicast Listener Report (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

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

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Multicast Listener Report v2 message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Neighbour Discovery Advertisement (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Neighbour Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbour Discovery Solicitation request.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Neighbour Discovery Solicitation (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Neighbour Discovery Solicitations are sent by nodes to discover the link-layer address of another on-link IPv6 node.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Packet Too Big (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Packet Too Big error messages are sent from any node that a packet traverses which is unable to forward the packet because the packet is too large for the next link.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Parameter Problem (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Parameter Problem error messages are sent by nodes as a result of incorrectly generated packets.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Router Advertisement (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Router Advertisement messages are sent by routers to other nodes for stateless auto-configuration.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	fe80::/64
Remote Addresses	LocalSubnet6 ff02::1 fe80::/64

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Router Solicitation (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Router Solicitation messages are sent by nodes seeking routers to provide stateless auto-configuration.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet6 ff02::2 fe80::/64

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Core Networking - Teredo (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound UDP rule to allow Teredo edge traversal, a technology that provides address assignment and automatic tunnelling for unicast IPv6 traffic when an IPv6/IPv4 host is located behind an IPv4 network address translator.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	Any

Core Networking - Time Exceeded (ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Time Exceeded error messages are generated from any node that a packet traverses if the Hop Limit value is decremented to zero at any point on the path.
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

Desktop App Web Viewer

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Desktop App Web Viewer
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Desktop App Web Viewer

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Desktop App Web Viewer
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Email and accounts

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Email and accounts
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Email and accounts

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Email and accounts
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

File and Printer Sharing (Echo Request - ICMPv4-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Echo Request messages are sent as ping requests to other nodes.
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv4
Local Ports	RPC
Remote Ports	Any

File and Printer Sharing (Echo Request - ICMPv6-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Echo Request messages are sent as ping requests to other nodes.
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	ICMPv6
Local Ports	RPC
Remote Ports	Any

File and Printer Sharing (LLMNR-UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for File and Printer Sharing to allow Link Local Multicast Name Resolution. [UDP 5355]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	5355

File and Printer Sharing (NB-Datagram-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for File and Printer Sharing to allow NetBIOS Datagram transmission and reception. [UDP 138]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	138

File and Printer Sharing (NB-Name-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for File and Printer Sharing to allow NetBIOS Name Resolution. [UDP 137]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	137

File and Printer Sharing (NB-Session-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for File and Printer Sharing to allow NetBIOS Session Service connections. [TCP 139]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	139

File and Printer Sharing (SMB-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for File and Printer Sharing to allow Server Message Block transmission and reception via Named Pipes. [TCP 445]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	445

mDNS (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for mDNS traffic [UDP]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	5353

mDNS (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for mDNS traffic [UDP]
Direction	Outbound
Enabled	True
Profile Names	Public

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	5353

mDNS (UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for mDNS traffic [UDP]
Direction	Outbound
Enabled	True
Profile Names	Domain

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	5353

Microsoft Media Foundation Network Source OUT [TCP ALL]

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	OutBound Rule for the Microsoft Media Foundation's Capture SVC to open TCP port to enable RTSP
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	554, 8554-8558

Narrator

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Narrator Home
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Narrator

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Narrator Home
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Network Discovery (LLMNR-UDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for Network Discovery to allow Link Local Multicast Name Resolution. [UDP 5355]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	5355

Network Discovery (NB-Datagram-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for Network Discovery to allow NetBIOS Datagram transmission and reception. [UDP 138]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	138

Network Discovery (NB-Name-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for Network Discovery to allow NetBIOS Name Resolution. [UDP 137]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	137

Network Discovery (Pub WSD-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for Network Discovery to discover devices via Function Discovery. [UDP 3702]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	3702

Network Discovery (SSDP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for Network Discovery to allow use of the Simple Service Discovery Protocol. [UDP 1900]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	1900

Network Discovery (UPnPHost-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for Network Discovery to allow use of Universal Plug and Play. [TCP]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	2869

Network Discovery (UPnP-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for Network Discovery to allow use of Universal Plug and Play. [TCP]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	2869

Network Discovery (WSD Events-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for Network Discovery to allow WSDAPI Events via Function Discovery. [TCP 5357]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	5357

Network Discovery (WSD EventsSecure-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	System
Description	Outbound rule for Network Discovery to allow Secure WSDAPI Events via Function Discovery. [TCP 5358]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	5358

Network Discovery (WSD-Out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Outbound rule for Network Discovery to discover devices via Function Discovery. [UDP 3702]
Direction	Outbound
Enabled	True
Profile Names	Private

Scope

Local Addresses	Any
Remote Addresses	LocalSubnet

Protocols and Ports

Protocol	UDP
Local Ports	Any
Remote Ports	3702

Start

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Start
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Start

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Start
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Default Lock Screen

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Default Lock Screen
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Default Lock Screen

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Default Lock Screen
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Defender SmartScreen

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Defender SmartScreen
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Defender SmartScreen

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Defender SmartScreen
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Device Management Certificate Installer (TCP out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\dmcertinst.exe
Description	Allow outbound TCP traffic from Windows Device Management Certificate Installer
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Windows Device Management Device Enroller (TCP out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\deviceenroller.exe
Description	Allow outbound TCP traffic from Windows Device Management Device Enroller
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	80, 443

Windows Device Management Enrolment Service (TCP out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\svchost.exe
Description	Allow outbound TCP traffic from Windows Device Management Enrolment Service
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Windows Device Management Sync Client (TCP out)

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	C:\Windows\system32\omadmclient.exe
Description	Allow outbound TCP traffic from Windows Device Management Sync Client
Direction	Outbound
Enabled	True
Profile Names	Any

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	TCP
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Feature Experience Pack

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Feature Experience Pack
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Search

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Search the web and Windows
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Search

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Search the web and Windows
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Security

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Security
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Security

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Security
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Shell Experience

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Shell Experience
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Shell Experience

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Shell Experience
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Shell Experience

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Shell Experience
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Shell Experience

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Windows Shell Experience
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Workplace or school account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Workplace or school account
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Workplace or school account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Workplace or school account
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Your account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Your account
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any

Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Your account

Provides details of the Windows Firewall rule.

General Settings

Source Type	Local
Action	Allow
Program	All programs that meet the specified conditions
Description	Your account
Direction	Outbound
Enabled	True
Profile Names	Domain, Private, Public

Scope

Local Addresses	Any
Remote Addresses	Any




Protocols and Ports

Protocol	Any
Local Ports	Any
Remote Ports	Any

Windows Patches

This section provides information about the system-wide updates (commonly referred to as a quick-fix engineering (QFE) updates) installed on this machine.

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\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.

```
<?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.ConnectionStringStringsSection, 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.xml.hosting" type="System.Xml.Hosting.Configuration.XamlHostingSectionGroup,
System.Xml.Hosting, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
  <section name="httpHandlers" type="System.Xml.Hosting.Configuration.XamlHostingSection, System.Xml.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" />
    </behaviorExtensions>
  </extensions>
</system.serviceModel>

```

```

    <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.SoopProcessingExtensionElement,
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
 Information	02 September 2022 12:33:46	Security-SPP	16384	None	N/A
 Information	02 September 2022 12:33:16	Security-SPP	16394	None	N/A
 Information	02 September 2022 12:25:08	VSS	8224	None	N/A
 Information	02 September 2022 12:18:10	SceCli	1704	None	N/A
 Information	02 September 2022 11:58:56	VSS	8224	None	N/A
 Information	02 September 2022 11:55:25	Security-SPP	16384	None	N/A
 Information	02 September 2022 11:54:56	SceCli	1704	None	N/A
 Information	02 September 2022 11:54:45	Security-SPP	16394	None	N/A
 Information	02 September 2022 11:53:32	Security-SPP	16384	None	N/A
 Information	02 September 2022 11:53:14	VSS	8224	None	N/A

02/09/2022 12:33:46

Date and Time	02 September 2022 12:33:46
Event ID	16,384
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Security-SPP
Task Category	None
Username	N/A
Message	Successfully scheduled Software Protection service for re-start at 2022-09-03T10:43:46Z. Reason: RulesEngine.

02/09/2022 12:33:16

Date and Time	02 September 2022 12:33:16
Event ID	16,394
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Security-SPP
Task Category	None
Username	N/A
Message	Offline downlevel migration succeeded.

i 02/09/2022 12:25:08

Date and Time	02 September 2022 12:25:08
Event ID	8,224
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	VSS
Task Category	None
Username	N/A
Message	The VSS service is shutting down due to idle timeout.

i 02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	1,704
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	SceCli
Task Category	None
Username	N/A
Message	Security policy in the Group policy objects has been applied successfully.

i 02/09/2022 11:58:56

Date and Time	02 September 2022 11:58:56
Event ID	8,224
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	VSS
Task Category	None
Username	N/A
Message	The VSS service is shutting down due to idle timeout.

i 02/09/2022 11:55:25

Date and Time	02 September 2022 11:55:25
Event ID	16,384
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Security-SPP
Task Category	None
Username	N/A
Message	Successfully scheduled Software Protection service for re-start at 2022-09-03T10:44:25Z. Reason: RulesEngine.

i 02/09/2022 11:54:56

Date and Time	02 September 2022 11:54:56
Event ID	1,704
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	SceCli
Task Category	None
Username	N/A
Message	Security policy in the Group policy objects has been applied successfully.

i 02/09/2022 11:54:45

Date and Time	02 September 2022 11:54:45
Event ID	16,394
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Security-SPP
Task Category	None
Username	N/A
Message	Offline downlevel migration succeeded.

i 02/09/2022 11:53:32

Date and Time	02 September 2022 11:53:32
Event ID	16,384
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Security-SPP
Task Category	None
Username	N/A
Message	Successfully scheduled Software Protection service for re-start at 2022-09-03T10:44:32Z. Reason: RulesEngine.

i 02/09/2022 11:53:14

Date and Time	02 September 2022 11:53:14
Event ID	8,224
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	VSS
Task Category	None
Username	N/A
Message	The VSS service is shutting down due to idle timeout.

Forwarded Events

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

Event Log Settings

Name	ForwardedEvents
Enabled	False
Classic Log	False
Log Path	%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx
Log Type	Operational
File Size	0 bytes
Record Count	0

File Access


Created	[Not Configured]
Last Accessed	[Not Configured]
Last Modified	[Not Configured]

Retention

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

Forwarded Events

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

 Most recent 0 entries

There are no event log entries found.

Hardware Events

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

Event Log Settings

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

File Access


Created	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

 02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$\br/>Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Kerberos Authentication Service Subcategory GUID: {0cce9242-69ae-11d9-bed3-505054503030} Changes: Success removed, Failure removed</p>

02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$ Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Other Account Logon Events Subcategory GUID: {0cce9241-69ae-11d9-bed3-505054503030} Changes: Success removed, Failure removed</p>

02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$ Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Kerberos Service Ticket Operations Subcategory GUID: {0cce9240-69ae-11d9-bed3-505054503030} Changes: Success removed, Failure removed</p>

02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$ Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Credential Validation Subcategory GUID: {0cce923f-69ae-11d9-bed3-505054503030} Changes: Failure removed</p>

02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$ Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Kerberos Authentication Service Subcategory GUID: {0cce9242-69ae-11d9-bed3-505054503030} Changes: Success Added, Failure added</p>

02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$\br/>Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Other Account Logon Events Subcategory GUID: {0cce9241-69ae-11d9-bed3-505054503030} Changes: Success Added, Failure added</p>

02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$\br/>Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Kerberos Service Ticket Operations Subcategory GUID: {0cce9240-69ae-11d9-bed3-505054503030} Changes: Success Added, Failure added</p>

02/09/2022 12:18:10

Date and Time	02 September 2022 12:18:10
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$ Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Credential Validation Subcategory GUID: {0cce923f-69ae-11d9-bed3-505054503030} Changes: Failure added</p>

02/09/2022 11:54:56

Date and Time	02 September 2022 11:54:56
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$ Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Kerberos Authentication Service Subcategory GUID: {0cce9242-69ae-11d9-bed3-505054503030} Changes: Success removed, Failure removed</p>

Date and Time	02 September 2022 11:54:56
Event ID	4,719
Entry Type	Success Audit
Machine Name	XCS-2K22.test2022.net
Source	Security-Auditing
Task Category	Audit Policy Change
Username	N/A
Message	<p>System audit policy was changed.</p> <p>Subject: Security ID: S-1-5-18 Account Name: XCS-2K22\$ Account Domain: TEST2022 Logon ID: 0x3E7</p> <p>Audit Policy Change: Category: Account Logon Subcategory: Other Account Logon Events Subcategory GUID: {0cce9241-69ae-11d9-bed3-505054503030} Changes: Success removed, Failure removed</p>

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

31/08/2022 16:48:27

Date and Time	31 August 2022 16:48:27
Event ID	9
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Selectable update File-Services of package FileServer-Core was successfully turned on.

31/08/2022 16:48:23

Date and Time	31 August 2022 16:48:23
Event ID	7
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Initiating changes to turn on update File-Services of package FileServer-Core. Client id: DISM Package Manager Provider.

i 31/05/2022 16:17:12

Date and Time	31 May 2022 16:17:12
Event ID	9
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Selectable update Microsoft-Windows-GroupPolicy-ServerAdminTools-Update of package GroupPolicy-ServerTools was successfully turned on.

i 31/05/2022 16:17:06

Date and Time	31 May 2022 16:17:06
Event ID	7
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Initiating changes to turn on update Microsoft-Windows-GroupPolicy-ServerAdminTools-Update of package GroupPolicy-ServerTools. Client id: DISM Package Manager Provider.

i 01/09/2021 16:33:47

Date and Time	01 September 2021 16:33:47
Event ID	9
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Selectable update WAS-WindowsActivationService of package IIS-WebServer-Core-Package was successfully turned on.

i 01/09/2021 16:33:47

Date and Time	01 September 2021 16:33:47
Event ID	9
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Selectable update WAS-ConfigurationAPI of package IIS-WebServer-Core-Package was successfully turned on.

i 01/09/2021 16:33:47

Date and Time	01 September 2021 16:33:47
Event ID	9
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Selectable update IIS-RequestMonitor of package IIS-WebServer-Core-Package was successfully turned on.

i 01/09/2021 16:33:47

Date and Time	01 September 2021 16:33:47
Event ID	9
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Selectable update IIS-ManagementService of package IIS-WebServer-Core-Package was successfully turned on.

i 01/09/2021 16:33:47

Date and Time	01 September 2021 16:33:47
Event ID	9
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Selectable update IIS-ApplicationInit of package IIS-WebServer-Core-Package was successfully turned on.

i 01/09/2021 16:33:37

Date and Time	01 September 2021 16:33:37
Event ID	7
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Servicing
Task Category	None
Username	NT AUTHORITY\SYSTEM
Message	Initiating changes to turn on update WAS-WindowsActivationService of package IIS-WebServer-Core-Package. Client id: DISM Package Manager Provider.

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

 02/09/2022 12:36:43

Date and Time	02 September 2022 12:36:43
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The AppX Deployment Service (AppXSVC) service entered the running state.

 02/09/2022 12:34:16

Date and Time	02 September 2022 12:34:16
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Windows Update Medic Service service entered the stopped state.

i 02/09/2022 12:33:55

Date and Time	02 September 2022 12:33:55
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Windows Biometric Service service entered the running state.

i 02/09/2022 12:33:55

Date and Time	02 September 2022 12:33:55
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Microsoft Passport Container service entered the running state.

i 02/09/2022 12:33:55

Date and Time	02 September 2022 12:33:55
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Microsoft Passport service entered the running state.

i 02/09/2022 12:33:46

Date and Time	02 September 2022 12:33:46
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Software Protection service entered the stopped state.

i 02/09/2022 12:33:16

Date and Time	02 September 2022 12:33:16
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Software Protection service entered the running state.

i 02/09/2022 12:33:16

Date and Time	02 September 2022 12:33:16
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Windows Update Medic Service service entered the running state.

i 02/09/2022 12:32:55

Date and Time	02 September 2022 12:32:55
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Windows Update service entered the stopped state.

i 02/09/2022 12:31:57

Date and Time	02 September 2022 12:31:57
Event ID	7,036
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	Service Control Manager
Task Category	None
Username	N/A
Message	The Background Intelligent Transfer Service service entered the stopped state.

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

Date and Time	02 September 2022 12:36:56
Event ID	800
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Pipeline Execution Details
Username	N/A
Message	<p>Pipeline execution details for command line: else { \$result = Add-Type -TypeDefinition \$securitySupportCoreSource }</p> <p>.</p> <p>Context Information: DetailSequence=1 DetailTotal=1</p> <p>SequenceNumber=281</p> <p>UserId=TEST2022\sysadmin HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion=5.1.20348.202 RunspaceId=76ac463f-c2ca-43b8-b838-50fef1ecb73c PipelineId=3 ScriptName= CommandLine=else { \$result = Add-Type -TypeDefinition \$securitySupportCoreSource }</p> <p>Details: CommandInvocation(Add-Type): "Add-Type" ParameterBinding(Add-Type): name="TypeDefinition"; value="using System; using System.Runtime.InteropServices; using System.Security.Principal; using System.Text;</p> <p>namespace CENTREL.XIA.Network.Management.Windows.SecuritySupportCore {</p> <p> /// <summary> /// Provides security support functions. /// </summary> public class SecuritySupportCore {</p> <p> /// <summary> /// The LookupAccountName function accepts the name of a system and an account as input. It retrieves a security identifier (SID) for the account and the name of the domain on which the account was found. /// </summary> /// <param name="systemName">The name of the system on which to execute the method.</param> /// <param name="accountName">The account name for which the SID should be obtained in the format "domain\username".</param> /// <param name="sid">A pointer to a buffer that receives the SID structure.</param> /// <param name="cbSid">A pointer to a variable. On input, this value specifies the size, in bytes, of the Sid buffer.</param> /// <param name="referencedDomainName">A pointer to a buffer that receives the name of the domain where the account name is found.</param> /// <param name="cbReferencedDomainName">A pointer to a variable. On input, this value specifies the size, in TCHARs, of the ReferencedDomainName buffer. </param> /// <param name="use">A pointer to a SID_NAME_USE enumerated type that indicates the type of the account when the function returns.</param> /// <returns>A System.Boolean value that indicates whether the method succeeded.</returns> /// <remarks>http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159(v=vs.8.5).aspx</remarks> [DllImport("advapi32.dll", CharSet = CharSet.Auto, SetLastError = true)] internal static extern bool LookupAccountName([In, MarshalAs(UnmanagedType.LPTStr)] string systemName, [In, MarshalAs(UnmanagedType.LPTStr)] string accountName, IntPtr sid, ref int cbSid, StringBuilder referencedDomainName, ref int cbReferencedDomainName,</p>

```

        out int use
    );

    /// <summary>
    /// Obtains the security identifier of the account name on the specified remote machine.
    /// </summary>
    /// <param name="machineName">The name of the remote system on which to perform the
resolution.</param>
    /// <param name="accountName">The name of the account to resolve in the format
"domain\username".</param>
    /// <returns>The security identifier on the remote machine in SDDL format.</returns>
    public static String GetAccountSid(String machineName, String accountName)
    {
        IntPtr sidPtr = IntPtr.Zero;
        try
        {
            int ERROR_INSUFFICIENT_BUFFER = 122;
            int ERROR_INVALID_FLAGS = 1004;
            int sidLength = 0;
            int domainLength = 0;
            int use = 0;
            StringBuilder domainName = new StringBuilder();
            int errorCode = 0;
            LookupAccountName(machineName, accountName, sidPtr, ref sidLength, domainName, ref
domainLength, out use);
            errorCode = Marshal.GetLastWin32Error();
            if (errorCode != ERROR_INSUFFICIENT_BUFFER && errorCode != ERROR_INVALID_FLAGS) { throw
new InvalidOperationException(String.Format("Error code {0}", errorCode)); }
            domainName = new StringBuilder(domainLength);
            sidPtr = Marshal.AllocHGlobal(sidLength);
            bool success = LookupAccountName(machineName, accountName, sidPtr, ref sidLength,
domainName, ref domainLength, out use);
            if (success)
            {
                SecurityIdentifier sid = new SecurityIdentifier(sidPtr);
                return sid.ToString();
            }
            errorCode = Marshal.GetLastWin32Error();
            throw new InvalidOperationException(String.Format("Error code {0}", errorCode));
        }
        catch (Exception ex) { throw new ArgumentException(String.Format("Could not get the SID for the account
name '{0}' on machine '{1}'. {2}", accountName, machineName, ex.Message), ex); }
        finally { Marshal.FreeHGlobal(sidPtr); }
    }
}
}
"

```

Date and Time	02 September 2022 12:36:56
Event ID	400
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Engine Lifecycle
Username	N/A
Message	<p>Engine state is changed from None to Available.</p> <p>Details: NewEngineState=Available PreviousEngineState=None</p> <p>SequenceNumber=279</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion=5.1.20348.202 RunspaceId=76ac463f-c2ca-43b8-b838-50fef1ecb73c PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>

Date and Time	02 September 2022 12:36:56
Event ID	600
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Provider Lifecycle
Username	N/A
Message	<p>Provider "WSMan" is Started.</p> <p>Details: ProviderName=WSMan NewProviderState=Started</p> <p>SequenceNumber=277</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>

Date and Time	02 September 2022 12:36:56
Event ID	600
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Provider Lifecycle
Username	N/A
Message	<p>Provider "Certificate" is Started.</p> <p>Details: ProviderName=Certificate NewProviderState=Started</p> <p>SequenceNumber=275</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>

Date and Time	02 September 2022 12:36:56
Event ID	600
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Provider Lifecycle
Username	N/A
Message	<p>Provider "Variable" is Started.</p> <p>Details: ProviderName=Variable NewProviderState=Started</p> <p>SequenceNumber=273</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>

Date and Time	02 September 2022 12:36:56
Event ID	600
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Provider Lifecycle
Username	N/A
Message	<p>Provider "Function" is Started.</p> <p>Details:</p> <p>ProviderName=Function NewProviderState=Started</p> <p>SequenceNumber=271</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>

Date and Time	02 September 2022 12:36:56
Event ID	600
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Provider Lifecycle
Username	N/A
Message	<p>Provider "FileSystem" is Started.</p> <p>Details:</p> <p>ProviderName=FileSystem NewProviderState=Started</p> <p>SequenceNumber=269</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>

Date and Time	02 September 2022 12:36:56
Event ID	600
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Provider Lifecycle
Username	N/A
Message	<p>Provider "Environment" is Started.</p> <p>Details: ProviderName=Environment NewProviderState=Started</p> <p>SequenceNumber=267</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>












Date and Time	02 September 2022 12:36:56
Event ID	600
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Provider Lifecycle
Username	N/A
Message	<p>Provider "Alias" is Started.</p> <p>Details: ProviderName=Alias NewProviderState=Started</p> <p>SequenceNumber=265</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>

Date and Time	02 September 2022 12:36:56
Event ID	600
Entry Type	Information
Machine Name	XCS-2K22.test2022.net
Source	PowerShell
Task Category	Provider Lifecycle
Username	N/A
Message	<p>Provider "Registry" is Started.</p> <p>Details:</p> <p>ProviderName=Registry NewProviderState=Started</p> <p>SequenceNumber=263</p> <p>HostName=Default Host HostVersion=5.1.20348.202 HostId=3ad33842-577a-437e-bc81-0be55a26c683 HostApplication=C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=</p>

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.





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	x86	3.80	2017.178.1.1	msodbcsql17.dll
 ODBC Driver 17 for SQL Server	x64	3.80	2017.178.1.1	msodbcsql17.dll
 SQL Server	x86	3.50	6.2.20348.1	SQLSRV32.dll
 SQL Server	x64	3.50	6.2.20348.1	SQLSRV32.dll
 SQL Server Native Client 11.0	x86	3.80	2011.110.7462.6	sqlncli11.dll
 SQL Server Native Client 11.0	x64	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

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)

Processes

Provides information about the processes that were running at the time of the scan.






































































































 139 Processes

Image Name	PID	CPU %	Memory (KB)	Description
 AggregatorHost.exe	3420	0	588	
 ApplicationFrameHost.exe	6944	0	3,704	Application Frame Host
 CENTREL.XIA.Configuration.Client.AdministrationTools.exe	7968	0	38,264	XIA Configuration Client Administration Tool
 CENTREL.XIA.Configuration.Server.Scheduler.exe	4924	0	12,224	CENTREL.XIA.Configuration.Server.Scheduler
 CENTREL.XIA.Configuration.Service.exe	3100	0	254,280	XIA Configuration Service
 chrome.exe	8012	0	52,128	Google Chrome
 chrome.exe	5592	0	7,508	Google Chrome
 chrome.exe	7292	0	1,252	Google Chrome
 chrome.exe	4432	0	8,476	Google Chrome
 chrome.exe	1584	0	61,208	Google Chrome
 chrome.exe	8808	0	4,716	Google Chrome
 chrome.exe	7204	0	110,856	Google Chrome
 chrome.exe	3464	0	2,756	Google Chrome
 conhost.exe	8832	0	3,328	Console Window Host
 csrss.exe	416	0	1,244	
 csrss.exe	528	0	1,108	
 ctfmon.exe	3152	0	3,372	CTF Loader
 dllhost.exe	6380	0	2,032	COM Surrogate
 dllhost.exe	3580	0	2,968	COM Surrogate
 dwm.exe	340	0	88,988	Desktop Window Manager

 explorer.exe	5164	0	40,260	Windows Explorer
 fontdrvhost.exe	796	0	3,136	Usermode Font Driver Host
 fontdrvhost.exe	804	0	2,540	Usermode Font Driver Host
 GoogleCrashHandler.exe	6752	0	72	Google Crash Handler
 GoogleCrashHandler64.exe	6764	0	20	Google Crash Handler
 lsass.exe	668	0	5,988	Local Security Authority Process
 mmc.exe	1620	0	62,212	Microsoft Management Console
 msdtc.exe	4320	0	2,104	Microsoft Distributed Transaction Coordinator Service
 msedge.exe	8908	0	1,280	Microsoft Edge
 msedge.exe	8684	0	41,796	Microsoft Edge
 msedge.exe	4044	0	7,000	Microsoft Edge
 msedge.exe	9208	0	16,016	Microsoft Edge
 msedge.exe	8476	0	6,320	Microsoft Edge
 msedge.exe	8572	0	2,836	Microsoft Edge
 msedge.exe	948	0	53,328	Microsoft Edge
 MsMpEng.exe	7348	0	151,520	
 NisSrv.exe	7888	0	2,180	
 powershell.exe	3820	0	21,012	Windows PowerShell
 procexp64.exe	3340	0	5,000	Sysinternals Process Explorer
 Registry	100	0	5,080	
 RuntimeBroker.exe	5780	0	1,660	Runtime Broker
 RuntimeBroker.exe	6016	0	4,732	Runtime Broker
 RuntimeBroker.exe	6200	0	2,272	Runtime Broker
 RuntimeBroker.exe	3352	0	2,772	Runtime Broker
 RuntimeBroker.exe	4688	0	2,744	Runtime Broker
 SearchApp.exe	5908	0	132	Search application

 SecurityHealthService.exe	7080	0	3,080	
 services.exe	636	0	5,792	
 ShellExperienceHost.exe	7664	0	56	Windows Shell Experience Host
 sihost.exe	4968	0	4,368	Shell Infrastructure Host
 smartscreen.exe	3472	0	5,192	Windows Defender SmartScreen
 smss.exe	292	0	284	
 spoolsv.exe	2128	0	4,372	Spooler SubSystem App
 sqlceip.exe	3084	0	24,720	Sql Server Telemetry Client
 sqlservr.exe	3092	32	195,512	SQL Server Windows NT - 64 Bit
 sqlwriter.exe	2488	0	1,184	SQL Server VSS Writer - 64 Bit
 StartMenuExperienceHost.exe	5616	0	14,568	
 svchost.exe	5148	0	1,208	Host Process for Windows Services
 svchost.exe	4504	0	1,056	Host Process for Windows Services
 svchost.exe	2468	0	2,096	Host Process for Windows Services
 svchost.exe	6828	0	1,948	Host Process for Windows Services
 svchost.exe	5040	0	4,984	Host Process for Windows Services
 svchost.exe	4976	0	2,528	Host Process for Windows Services
 svchost.exe	6260	0	1,836	Host Process for Windows Services
 svchost.exe	5924	0	3,316	Host Process for Windows Services
 svchost.exe	6628	0	2,784	Host Process for Windows Services
 svchost.exe	3884	0	924	Host Process for Windows Services
 svchost.exe	9152	0	5,844	Host Process for Windows Services
 svchost.exe	7556	0	1,620	Host Process for Windows Services
 svchost.exe	7964	0	3,440	Host Process for Windows Services
 svchost.exe	1008	0	1,948	Host Process for Windows Services
 svchost.exe	3332	0	3,920	Host Process for Windows Services

 svchost.exe	7024	0	1,024	Host Process for Windows Services
 svchost.exe	1812	0	2,260	Host Process for Windows Services
 svchost.exe	1680	0	4,384	Host Process for Windows Services
 svchost.exe	1668	0	856	Host Process for Windows Services
 svchost.exe	1652	0	2,460	Host Process for Windows Services
 svchost.exe	1632	0	2,580	Host Process for Windows Services
 svchost.exe	1528	0	3,292	Host Process for Windows Services
 svchost.exe	1492	0	3,412	Host Process for Windows Services
 svchost.exe	1480	0	8,452	Host Process for Windows Services
 svchost.exe	1368	0	15,640	Host Process for Windows Services
 svchost.exe	1272	0	2,280	Host Process for Windows Services
 svchost.exe	1256	0	968	Host Process for Windows Services
 svchost.exe	1204	0	1,556	Host Process for Windows Services
 svchost.exe	1196	0	1,160	Host Process for Windows Services
 svchost.exe	1132	0	1,236	Host Process for Windows Services
 svchost.exe	1116	0	1,532	Host Process for Windows Services
 svchost.exe	1056	0	1,232	Host Process for Windows Services
 svchost.exe	896	0	2,940	Host Process for Windows Services
 svchost.exe	648	0	820	Host Process for Windows Services
 svchost.exe	784	0	1,032	Host Process for Windows Services
 svchost.exe	940	0	1,760	Host Process for Windows Services
 svchost.exe	880	0	5,704	Host Process for Windows Services
 svchost.exe	768	0	5,928	Host Process for Windows Services
 svchost.exe	8920	0	2,796	
 svchost.exe	4188	0	1,768	Host Process for Windows Services
 svchost.exe	1880	0	1,396	Host Process for Windows Services

 svchost.exe	1836	0	1,404	Host Process for Windows Services
 svchost.exe	2000	0	1,328	Host Process for Windows Services
 svchost.exe	3688	0	1,348	Host Process for Windows Services
 svchost.exe	2800	0	2,468	Host Process for Windows Services
 svchost.exe	4232	0	1,268	Host Process for Windows Services
 svchost.exe	2768	0	1,100	Host Process for Windows Services
 svchost.exe	2716	0	2,496	Host Process for Windows Services
 svchost.exe	2704	0	12,400	Host Process for Windows Services
 svchost.exe	2696	0	3,708	Host Process for Windows Services
 svchost.exe	5736	0	1,208	Host Process for Windows Services
 svchost.exe	1936	0	1,612	Host Process for Windows Services
 svchost.exe	2556	0	1,088	Host Process for Windows Services
 svchost.exe	2604	0	836	Host Process for Windows Services
 svchost.exe	2528	0	6,012	Host Process for Windows Services
 svchost.exe	2480	0	1,712	Host Process for Windows Services
 svchost.exe	2424	0	1,216	Host Process for Windows Services
 svchost.exe	2300	0	12,320	Host Process for Windows Services
 svchost.exe	2256	0	820	Host Process for Windows Services
 svchost.exe	2248	0	2,528	Host Process for Windows Services
 svchost.exe	2192	0	3,344	Host Process for Windows Services
 svchost.exe	2168	0	1,496	Host Process for Windows Services
 svchost.exe	2152	0	2,044	Host Process for Windows Services
 svchost.exe	2044	0	1,428	Host Process for Windows Services
 System	4	0	12	
 System Idle Process	0	68	8	
 taskhostw.exe	3604	0	1,980	Host Process for Windows Tasks

 Taskmgr.exe	7252	0	17,212	Task Manager
 TextInputHost.exe	5584	0	6,952	
 VGAuthService.exe	2628	0	2,236	VMware Guest Authentication Service
 vm3dservice.exe	4020	0	988	VMware SVGA Helper Service
 vm3dservice.exe	2880	0	984	VMware SVGA Helper Service
 vm3dservice.exe	2644	0	956	VMware SVGA Helper Service
 vmttoolsd.exe	2660	0	7,896	VMware Tools Core Service
 vmttoolsd.exe	7692	0	15,512	VMware Tools Core Service
 w3wp.exe	4900	0	410,224	IIS Worker Process
 wininit.exe	512	0	784	
 winlogon.exe	604	0	1,424	Windows Log-on Application
 WmiPrvSE.exe	8156	0	29,544	WMI Provider Host
 WmiPrvSE.exe	6228	0	5,428	WMI Provider Host
 WmiPrvSE.exe	3752	0	12,608	WMI Provider Host
 WmiPrvSE.exe	4736	0	4,732	WMI Provider Host

Registry

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

1 Registry Keys

Display Name	Registry Hive	Located
 XIA Configuration Server Setup	HKEY_LOCAL_MACHINE	True

1 Registry Values

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

XIA Configuration Server Setup

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

Registry Key

Located	True
---------	------

Registry Key Properties

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

12 Values


Name	Value Type	Data
Account	REG_SZ	NT AUTHORITY\NETWORK SERVICE
AddUserSystemAdministrator	REG_SZ	True
AuthenticationMode	REG_SZ	NETWORKSERVICE
DatabaseInstance	REG_SZ	(local)\SQLEXPRESS
DatabaseName	REG_SZ	XIAConfiguration
Domain	REG_SZ	NT AUTHORITY
InstallDirectory	REG_SZ	C:\Program Files\CENTREL Solutions\XIA Configuration\
OrganizationName	REG_SZ	Demonstration Company
URL	REG_SZ	http://localhost/XIAConfiguration
Username	REG_SZ	NETWORK SERVICE
Version	REG_SZ	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-1-15-3-1024-106536593-6-1281604716-351173842-8-1654721687-432734479	True	Allow	Read	This key and subkeys

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

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

<input type="checkbox"/> Message Queuing Triggers	Available
<input type="checkbox"/> Multicasting Support	Available
<input type="checkbox"/> Routing Service	Available
<input checked="" type="checkbox"/> Microsoft Defender Antivirus	Installed
<input type="checkbox"/> Multipath I/O	Available
<input type="checkbox"/> MultiPoint Connector	Available
<input type="checkbox"/> MultiPoint Connector Services	Available
<input type="checkbox"/> MultiPoint Manager and MultiPoint Dashboard	Available
<input type="checkbox"/> Network Controller	Available
<input type="checkbox"/> Network Load Balancing	Available
<input type="checkbox"/> Network Policy and Access Services	Available
<input type="checkbox"/> Network Virtualization	Available
<input type="checkbox"/> Peer Name Resolution Protocol	Available
<input type="checkbox"/> Print and Document Services	Available
<input type="checkbox"/> Internet Printing	Available
<input type="checkbox"/> LPD Service	Available
<input type="checkbox"/> Print Server	Available
<input type="checkbox"/> Quality Windows Audio Video Experience	Available
<input type="checkbox"/> RAS Connection Manager Administration Kit (CMAK)	Available
<input type="checkbox"/> Remote Access	Available
<input type="checkbox"/> DirectAccess and VPN (RAS)	Available
<input type="checkbox"/> Routing	Available
<input type="checkbox"/> Web Application Proxy	Available
<input type="checkbox"/> Remote Assistance	Available
<input type="checkbox"/> Remote Desktop Services	Available
<input type="checkbox"/> Remote Desktop Connection Broker	Available
<input type="checkbox"/> Remote Desktop Gateway	Available
<input type="checkbox"/> Remote Desktop Licensing	Available
<input type="checkbox"/> Remote Desktop Session Host	Available
<input type="checkbox"/> Remote Desktop Virtualization Host	Available
<input type="checkbox"/> Remote Desktop Web Access	Available
<input type="checkbox"/> Remote Differential Compression	Available
<input type="checkbox"/> Remote Server Administration Tools	Available
<input type="checkbox"/> Feature Administration Tools	Available
<input type="checkbox"/> BitLocker Drive Encryption Administration Utilities	Available
<input type="checkbox"/> BitLocker Drive Encryption Tools	Available
<input type="checkbox"/> BitLocker Recovery Password Viewer	Available
<input type="checkbox"/> BITS Server Extensions Tools	Available
<input type="checkbox"/> DataCenterBridging LLDP Tools	Available
<input type="checkbox"/> Failover Clustering Tools	Available

<input type="checkbox"/> Failover Cluster Automation Server	Available
<input type="checkbox"/> Failover Cluster Command Interface	Available
<input type="checkbox"/> Failover Cluster Management Tools	Available
<input type="checkbox"/> Failover Cluster Module for Windows PowerShell	Available
<input type="checkbox"/> IP Address Management (IPAM) Client	Available
<input type="checkbox"/> Network Load Balancing Tools	Available
<input type="checkbox"/> Shielded VM Tools	Available
<input type="checkbox"/> SMTP Server Tools	Available
<input type="checkbox"/> SNMP Tools	Available
<input type="checkbox"/> Storage Migration Service Tools	Available
<input type="checkbox"/> Storage Replica Module for Windows PowerShell	Available
<input type="checkbox"/> System Insights Module for Windows PowerShell	Available
<input type="checkbox"/> WINS Server Tools	Available
<input type="checkbox"/> Role Administration Tools	Available
<input type="checkbox"/> Active Directory Certificate Services Tools	Available
<input type="checkbox"/> Certification Authority Management Tools	Available
<input type="checkbox"/> Online Responder Tools	Available
<input type="checkbox"/> Active Directory Rights Management Services Tools	Available
<input type="checkbox"/> AD DS and AD LDS Tools	Available
<input type="checkbox"/> Active Directory module for Windows PowerShell	Available
<input type="checkbox"/> AD DS Tools	Available
<input type="checkbox"/> Active Directory Administrative Center	Available
<input type="checkbox"/> AD DS Snap-Ins and Command-Line Tools	Available
<input type="checkbox"/> AD LDS Snap-Ins and Command-Line Tools	Available
<input type="checkbox"/> DHCP Server Tools	Available
<input type="checkbox"/> DNS Server Tools	Available
<input type="checkbox"/> Fax Server Tools	Available
<input type="checkbox"/> File Services Tools	Available
<input type="checkbox"/> DFS Management Tools	Available
<input type="checkbox"/> File Server Resource Manager Tools	Available
<input type="checkbox"/> Services for Network File System Management Tools	Available
<input type="checkbox"/> Hyper-V Management Tools	Available
<input type="checkbox"/> Hyper-V GUI Management Tools	Available
<input type="checkbox"/> Hyper-V Module for Windows PowerShell	Available
<input type="checkbox"/> Network Controller Management Tools	Available
<input type="checkbox"/> Network Policy and Access Services Tools	Available
<input type="checkbox"/> Print and Document Services Tools	Available
<input type="checkbox"/> Remote Access Management Tools	Available
<input type="checkbox"/> Remote Access GUI and Command-Line Tools	Available
<input type="checkbox"/> Remote Access module for Windows PowerShell	Available

<input type="checkbox"/> Remote Desktop Services Tools	Available
<input type="checkbox"/> Remote Desktop Gateway Tools	Available
<input type="checkbox"/> Remote Desktop Licensing Diagnoser Tools	Available
<input type="checkbox"/> Remote Desktop Licensing Tools	Available
<input type="checkbox"/> Volume Activation Tools	Available
<input type="checkbox"/> Windows Deployment Services Tools	Available
<input type="checkbox"/> Windows Server Update Services Tools	Available
<input type="checkbox"/> API and PowerShell cmdlets	Available
<input type="checkbox"/> User Interface Management Console	Available
<input type="checkbox"/> RPC over HTTP Proxy	Available
<input type="checkbox"/> Setup and Boot Event Collection	Available
<input type="checkbox"/> Simple TCP/IP Services	Available
<input type="checkbox"/> SMB 1.0/CIFS File Sharing Support	Available
<input type="checkbox"/> SMB 1.0/CIFS Client	Available
<input type="checkbox"/> SMB 1.0/CIFS Server	Available
<input type="checkbox"/> SMB Bandwidth Limit	Available
<input type="checkbox"/> SMTP Server	Available
<input type="checkbox"/> SNMP Service	Available
<input type="checkbox"/> SNMP WMI Provider	Available
<input type="checkbox"/> Software Load Balancer	Available
<input type="checkbox"/> Storage Migration Service	Available
<input type="checkbox"/> Storage Migration Service Proxy	Available
<input type="checkbox"/> Storage Replica	Available
<input checked="" type="checkbox"/> System Data Archiver	Installed
<input type="checkbox"/> System Insights	Available
<input type="checkbox"/> Telnet Client	Available
<input type="checkbox"/> TFTP Client	Available
<input type="checkbox"/> VM Shielding Tools for Fabric Management	Available
<input type="checkbox"/> Volume Activation Services	Available
<input checked="" type="checkbox"/> Web Server (IIS)	Installed
<input type="checkbox"/> FTP Server	Available
<input type="checkbox"/> FTP Extensibility	Available
<input type="checkbox"/> FTP Service	Available
<input checked="" type="checkbox"/> Management Tools	Installed
<input type="checkbox"/> IIS 6 Management Compatibility	Available
<input type="checkbox"/> IIS 6 Management Console	Available
<input type="checkbox"/> IIS 6 Metabase Compatibility	Available
<input type="checkbox"/> IIS 6 Scripting Tools	Available
<input type="checkbox"/> IIS 6 WMI Compatibility	Available
<input checked="" type="checkbox"/> IIS Management Console	Installed

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

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

<input type="checkbox"/> Netlogon	Automatic	LocalSystem
<input type="checkbox"/> Network Connection Broker	Manual (Trigger Start)	LocalSystem
<input type="checkbox"/> Network Connections	Manual	LocalSystem
<input type="checkbox"/> Network Connectivity Assistant	Manual (Trigger Start)	LocalSystem
<input type="checkbox"/> Network List Service	Manual	NT AUTHORITY\LocalService
<input type="checkbox"/> Network Location Awareness	Automatic	NT AUTHORITY\NetworkService
<input type="checkbox"/> Network Setup Service	Manual (Trigger Start)	LocalSystem
<input type="checkbox"/> Network Store Interface Service	Automatic	NT Authority\LocalService
<input checked="" type="checkbox"/> Offline Files	Disabled	LocalSystem
<input checked="" type="checkbox"/> OpenSSH Authentication Agent	Disabled	LocalSystem
<input type="checkbox"/> Optimise drives	Manual	localSystem
<input checked="" type="checkbox"/> Payments and NFC/SE Manager	Disabled	NT AUTHORITY\LocalService
<input type="checkbox"/> Performance Counter DLL Host	Manual	NT AUTHORITY\LocalService
<input type="checkbox"/> Performance Logs & Alerts	Manual	NT AUTHORITY\LocalService
<input type="checkbox"/> PimIndexMaintenanceSvc_526cb	Manual	
<input type="checkbox"/> Plug and Play	Manual	LocalSystem
<input type="checkbox"/> Portable Device Enumerator Service	Manual (Trigger Start)	LocalSystem
<input type="checkbox"/> Power	Automatic	LocalSystem
<input type="checkbox"/> Print Spooler	Automatic	LocalSystem
<input type="checkbox"/> Printer Extensions and Notifications	Manual	LocalSystem
<input type="checkbox"/> PrintWorkflowUserSvc_526cb	Manual (Trigger Start)	
<input type="checkbox"/> Problem Reports Control Panel Support	Manual	localSystem
<input type="checkbox"/> Program Compatibility Assistant Service	Automatic (Delayed Start, Trigger Start)	LocalSystem
<input type="checkbox"/> Quality Windows Audio Video Experience	Manual	NT AUTHORITY\LocalService
<input checked="" type="checkbox"/> Radio Management Service	Disabled	NT AUTHORITY\LocalService
<input type="checkbox"/> 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 Services [A - I]

Displays the configuration of the Windows services on this machine

ActiveX Installer (AxInstSV)

Name	AxInstSV
Display Name	ActiveX Installer (AxInstSV)
Description	Provides User Account Control validation for the installation of ActiveX controls from the Internet and enables management of ActiveX control installation based on Group Policy settings. This service is started on demand and if disabled the installation of ActiveX controls will behave according to default browser settings.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k AxInstSVGroup
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

AllJoyn Router Service

Name	AJRouter
Display Name	AllJoyn Router Service
Description	Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled routers will be unable to run.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies


Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 App Readiness

Name	AppReadiness
Display Name	App Readiness
Description	Gets apps ready for use the first time a user signs in to this PC and when adding new apps.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k AppReadiness -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Application Host Helper Service

Name	AppHostSvc
Display Name	Application Host Helper Service
Description	Provides administrative services for IIS, for example configuration history and Application Pool account mapping. If this service is stopped, configuration history and locking down files or directories with Application Pool specific Access Control Entries will not work.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k apphost
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Application Identity

Name	AppIDSvc
Display Name	Application Identity
Description	Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs AppID CryptSvc
--------------------	----------------------------

Log On

Account Name	NT Authority\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Application Information

Name	Appinfo
Display Name	Application Information
Description	Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform desired user tasks.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies


Service Depends On	RpcSs ProfSvc
--------------------	------------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Application Layer Gateway Service

Name	ALG
Display Name	Application Layer Gateway Service
Description	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\alg.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Application Management

Name	AppMgmt
Display Name	Application Management
Description	Processes installation, removal and enumeration requests for software deployed through Group Policy. If the service is disabled, users will be unable to install, remove or enumerate software deployed through Group Policy. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

AppX Deployment Service (AppXSVC)

Name	AppXSvc
Display Name	AppX Deployment Service (AppXSVC)
Description	Provides infrastructure support for deploying Store applications. This service is started on demand and if disabled Store applications will not be deployed to the system, and may not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k wsappx -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	rpcss staterepository
--------------------	--------------------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

ASP.NET State Service

Name	aspnet_state
Display Name	ASP.NET State Service
Description	Provides support for out-of-process session states for ASP.NET. If this service is stopped, out-of-process requests will not be processed. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Auto Time Zone Updater


Name	tzautoupdate
Display Name	Auto Time Zone Updater
Description	Automatically sets the system time zone.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On


Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

 AzureAttestService

Name	AzureAttestService
Display Name	AzureAttestService
Description	

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k AzureAttestService
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Background Intelligent Transfer Service

Name	BITS
Display Name	Background Intelligent Transfer Service
Description	Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN Explorer, will be unable to automatically download programs and other information.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Background Tasks Infrastructure Service

Name	BrokerInfrastructure
Display Name	Background Tasks Infrastructure Service
Description	Windows infrastructure service that controls which background tasks can run on the system.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcEptMapper DcomLaunch RpcSs
--------------------	-------------------------------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Restart the Computer
Subsequent Failure Action	Restart the Computer
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	2 minutes

Base Filtering Engine

Name	BFE
Display Name	Base Filtering Engine
Description	The Base Filtering Engine (BFE) is a service that manages firewall and Internet Protocol security (IPsec) policies and implements user mode filtering. Stopping or disabling the BFE service will significantly reduce the security of the system. It will also result in unpredictable behavior in IPsec management and firewall applications.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Bluetooth Support Service

Name	bthserv
Display Name	Bluetooth Support Service
Description	The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed Bluetooth devices to fail to operate properly and prevent new devices from being discovered or associated.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Capability Access Manager Service

Name	camsvc
Display Name	Capability Access Manager Service
Description	Provides facilities for managing UWP apps access to app capabilities as well as checking an app's access to specific app capabilities

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k appmodel -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

☰ CaptureService_526cb

Name	CaptureService_526cb
Display Name	CaptureService_526cb
Description	Enables optional screen capture functionality for applications that call the Windows.Graphics.Capture API.

🔧 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

🔗 Dependencies

Service Depends On	
--------------------	--

👤 Log On

Account Name	
--------------	--

🔄 Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

CDPUserSvc_526cb

Name	CDPUserSvc_526cb
Display Name	CDPUserSvc_526cb
Description	This user service is used for Connected Devices Platform scenarios

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	
--------------	--

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Certificate Propagation

Name	CertPropSvc
Display Name	Certificate Propagation
Description	Copies user certificates and root certificates from smart cards into the current user's certificate store, detects when a smart card is inserted into a smart card reader, and, if needed, installs the smart card Plug and Play minidriver.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Client Licence Service (ClipSVC)

Name	ClipSVC
Display Name	Client Licence Service (ClipSVC)
Description	Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled applications bought using Windows Store will not behave correctly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k wsappx -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

CNG Key Isolation

Name	KeyIso
Display Name	CNG Key Isolation
Description	The CNG key isolation service is hosted in the LSA process. The service provides key process isolation to private keys and associated cryptographic operations as required by the Common Criteria. The service stores and uses long-lived keys in a secure process complying with Common Criteria requirements.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\lsass.exe
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

COM+ Event System

Name	EventSystem
Display Name	COM+ Event System
Description	Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. If the service is stopped, SENS will close and will not be able to provide logon and logoff notifications. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

COM+ System Application

Name	COMSysApp
Display Name	COM+ System Application
Description	Manages the configuration and tracking of Component Object Model (COM)+-based components. If the service is stopped, most COM+-based components will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\dlhhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	RpcSs EventSystem SENS
--------------------	------------------------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Connected Devices Platform Service

Name	CDPsvc
Display Name	Connected Devices Platform Service
Description	This service is used for Connected Devices Platform scenarios

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Running

Dependencies

Service Depends On	ncbservice RpcSS Tcpip
--------------------	------------------------------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

☰ Connected User Experiences and Telemetry

Name	DiagTrack
Display Name	Connected User Experiences and Telemetry
Description	The Connected User Experiences and Telemetry service enables features that support in-application and connected user experiences. Additionally, this service manages the event driven collection and transmission of diagnostic and usage information (used to improve the experience and quality of the Windows Platform) when the diagnostics and usage privacy option settings are enabled under Feedback and Diagnostics.

🔑 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k utcsvc -p
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

🔗 Dependencies

Service Depends On	RpcSs
--------------------	-------

👤 Log On

Account Name	LocalSystem
--------------	-------------

🔄 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

ConsentUxUserSvc_526cb


Name	ConsentUxUserSvc_526cb
Display Name	ConsentUxUserSvc_526cb
Description	Allows the system to request user consent to allow apps to access sensitive resources and information such as the device's location

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DevicesFlow
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On


Account Name	
--------------	--

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 CoreMessaging


Name	CoreMessagingRegistrar
Display Name	CoreMessaging
Description	Manages communication between system components.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies


Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery


First Failure Action	Restart the Computer
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	True
Computer Restart Delay	0 minutes

 Credential Manager

Name	VaultSvc
Display Name	Credential Manager
Description	Provides secure storage and retrieval of credentials to users, applications and security service packages.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\lsass.exe
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 CredentialEnrollmentManagerUserSvc_526cb

Name	CredentialEnrollmentManagerUserSvc_526cb
Display Name	CredentialEnrollmentManagerUserSvc_526cb
Description	Credential Enrollment Manager

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\CredentialEnrollmentManager.exe
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	
--------------	--

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Cryptographic Services

Name	CryptSvc
Display Name	Cryptographic Services
Description	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as SSL. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	NT Authority\NetworkService
--------------	-----------------------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 Data Sharing Service


Name	DsSvc
Display Name	Data Sharing Service
Description	Provides data brokering between applications.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 DCOM Server Process Launcher

Name	DcomLaunch
Display Name	DCOM Server Process Launcher
Description	The DCOMLAUNCH service launches COM and DCOM servers in response to object activation requests. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the DCOMLAUNCH service running.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies


Service Depends On	
--------------------	--

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Computer
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	1 minutes

 Delivery Optimization


Name	DoSvc
Display Name	Delivery Optimization
Description	Performs content delivery optimization tasks

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	NT Authority\NetworkService
--------------	-----------------------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

☰ Device Association Service

Name	DeviceAssociationService
Display Name	Device Association Service
Description	Enables pairing between the system and wired or wireless devices.

🔑 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

🔗 Dependencies

Service Depends On	
--------------------	--

👤 Log On

Account Name	LocalSystem
--------------	-------------

🔄 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Device Install Service

Name	DeviceInstall
Display Name	Device Install Service
Description	Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies


Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	True

 Device Management Enrollment Service

Name	DmEnrollmentSvc
Display Name	Device Management Enrollment Service
Description	Performs Device Enrollment Activities for Device Management

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Device Management Wireless Application Protocol (WAP) Push message Routing Service


Name	dmwappushservice
Display Name	Device Management Wireless Application Protocol (WAP) Push message Routing Service
Description	Routes Wireless Application Protocol (WAP) Push messages received by the device and synchronizes Device Management sessions

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Device Setup Manager

Name	DsmSvc
Display Name	Device Setup Manager
Description	Enables the detection, download and installation of device-related software. If this service is disabled, devices may be configured with outdated software, and may not work correctly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

DeviceAssociationBrokerSvc_526cb

Name	DeviceAssociationBrokerSvc_526cb
Display Name	DeviceAssociationBrokerSvc_526cb
Description	Enables apps to pair devices

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DevicesFlow -p
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	
--------------	--

Recovery


First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 DevicePickerUserSvc_526cb

Name	DevicePickerUserSvc_526cb
Display Name	DevicePickerUserSvc_526cb
Description	This user service is used for managing the Miracast, DLNA and DIAL UI

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DevicesFlow
Service Execution Type	Unknown
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	
--------------	--

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

🔍 DevicesFlowUserSvc_526cb

Name	DevicesFlowUserSvc_526cb
Display Name	DevicesFlowUserSvc_526cb
Description	Allows ConnectUX and PC Settings to Connect and Pair with WiFi displays and Bluetooth devices.

🔑 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DevicesFlow
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

🔗 Dependencies

Service Depends On	
--------------------	--

👤 Log On

Account Name	
--------------	--

🔄 Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

DevQuery Background Discovery Broker

Name	DevQueryBroker
Display Name	DevQuery Background Discovery Broker
Description	Enables apps to discover devices with a background task

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

DHCP Client

Name	Dhcp
Display Name	DHCP Client
Description	Registers and updates IP addresses and DNS records for this computer. If this service is stopped, this computer will not receive dynamic IP addresses and DNS updates. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	NSI Afd
--------------------	------------

Log On

Account Name	NT Authority\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Diagnostic Policy Service

Name	DPS
Display Name	Diagnostic Policy Service
Description	The Diagnostic Policy Service enables problem detection, troubleshooting and resolution for Windows components. If this service is stopped, diagnostics will no longer function.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Diagnostic Service Host

Name	WdiServiceHost
Display Name	Diagnostic Service Host
Description	The Diagnostic Service Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local Service context. If this service is stopped, any diagnostics that depend on it will no longer function.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Diagnostic System Host

Name	WdiSystemHost
Display Name	Diagnostic System Host
Description	The Diagnostic System Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local System context. If this service is stopped, any diagnostics that depend on it will no longer function.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Display Policy Service

Name	DispBrokerDesktopSvc
Display Name	Display Policy Service
Description	Manages the connection and configuration of local and remote displays

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

 Dependencies

Service Depends On	RpcSS
--------------------	-------

 Log On


Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Distributed Link Tracking Client

Name	TrkWks
Display Name	Distributed Link Tracking Client
Description	Maintains links between NTFS files within a computer or across computers in a network.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Distributed Transaction Coordinator

Name	MSDTC
Display Name	Distributed Transaction Coordinator
Description	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will fail. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\msdtc.exe
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies

Service Depends On	RPCSS SamSS
--------------------	----------------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

DNS Client

Name	Dnscache
Display Name	DNS Client
Description	The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer's name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies


Service Depends On	nsi Afd
--------------------	------------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Downloaded Maps Manager


Name	MapsBroker
Display Name	Downloaded Maps Manager
Description	Windows service for application access to downloaded maps. This service is started on-demand by applications accessing downloaded maps. Disabling this service will prevent apps from accessing maps.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetworkService -p
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies


Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Embedded Mode


Name	embeddedmode
Display Name	Embedded Mode
Description	The Embedded Mode service enables scenarios related to Background Applications. Disabling this service will prevent Background Applications from being activated.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies

Service Depends On	BrokerInfrastructure
--------------------	----------------------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Encrypting File System (EFS)

Name	EFS
Display Name	Encrypting File System (EFS)
Description	Provides the core file encryption technology used to store encrypted files on NTFS file system volumes. If this service is stopped or disabled, applications will be unable to access encrypted files.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\lsass.exe
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Enterprise App Management Service

Name	EntAppSvc
Display Name	Enterprise App Management Service
Description	Enables enterprise application management.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k appmodel -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Extensible Authentication Protocol

Name	EapHost
Display Name	Extensible Authentication Protocol
Description	The Extensible Authentication Protocol (EAP) service provides network authentication in such scenarios as 802.1x wired and wireless, VPN, and Network Access Protection (NAP). EAP also provides application programming interfaces (APIs) that are used by network access clients, including wireless and VPN clients, during the authentication process. If you disable this service, this computer is prevented from accessing networks that require EAP authentication.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS KeyIso
--------------------	-----------------

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Function Discovery Provider Host

Name	fdPHost
Display Name	Function Discovery Provider Host
Description	The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD providers supply network discovery services for the Simple Services Discovery Protocol (SSDP) and Web Services – Discovery (WS-D) protocol. Stopping or disabling the FDPHOST service will disable network discovery for these protocols when using FD. When this service is unavailable, network services using FD and relying on these discovery protocols will be unable to find network devices or resources.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs http
--------------------	---------------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Function Discovery Resource Publication

Name	FDResPub
Display Name	Function Discovery Resource Publication
Description	Publishes this computer and resources attached to this computer so they can be discovered over the network. If this service is stopped, network resources will no longer be published and they will not be discovered by other computers on the network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs http fdphost
--------------------	--------------------------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Geolocation Service

Name	lfsvc
Display Name	Geolocation Service
Description	This service monitors the current location of the system and manages geofences (a geographical location with associated events). If you turn off this service, applications will be unable to use or receive notifications for geolocation or geofences.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Google Chrome Elevation Service (GoogleChromeElevationService)

Name	GoogleChromeElevationService
Display Name	Google Chrome Elevation Service (GoogleChromeElevationService)
Description	

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Google\Chrome\Application\104.0.5112.102\elevation_service.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Google Update Service (gupdate)

Name	gupdate
Display Name	Google Update Service (gupdate)
Description	Keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start)
Service State	Stopped

Dependencies


Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Google Update Service (gupdatem)


Name	gupdatem
Display Name	Google Update Service (gupdatem)
Description	Keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	RPCSS
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 GraphicsPerfSvc

Name	GraphicsPerfSvc
Display Name	GraphicsPerfSvc
Description	Graphics performance monitor service

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k GraphicsPerfSvcGroup
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	1440 minutes
Enable Actions for Stops with Errors	False

Group Policy Client

Name	gpsvc
Display Name	Group Policy Client
Description	The service is responsible for applying settings configured by administrators for the computer and users through the Group Policy component. If the service is disabled, the settings will not be applied and applications and components will not be manageable through Group Policy. Any components or applications that depend on the Group Policy component might not be functional if the service is disabled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k GPSvcGroup
Service Execution Type	Own Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RPCSS Mup
--------------------	--------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Human Interface Device Service

Name	hidserv
Display Name	Human Interface Device Service
Description	Activates and maintains the use of hot buttons on keyboards, remote controls and other multimedia devices. It is recommended that you keep this service running.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies


Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 HV Host Service

Name	HvHost
Display Name	HV Host Service
Description	Provides an interface for the Hyper-V hypervisor to provide per-partition performance counters to the host operating system.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies

Service Depends On	hvservice
--------------------	-----------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Hyper-V Data Exchange Service

Name	vmickvpexchange
Display Name	Hyper-V Data Exchange Service
Description	Provides a mechanism to exchange data between the virtual machine and the operating system running on the physical computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Hyper-V Guest Service Interface

Name	vmicguestinterface
Display Name	Hyper-V Guest Service Interface
Description	Provides an interface for the Hyper-V host to interact with specific services running inside the virtual machine.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Hyper-V Guest Shutdown Service

Name	vmicshUTDOWN
Display Name	Hyper-V Guest Shutdown Service
Description	Provides a mechanism to shut down the operating system of this virtual machine from the management interfaces on the physical computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Hyper-V Heartbeat Service

Name	vmicheartbeat
Display Name	Hyper-V Heartbeat Service
Description	Monitors the state of this virtual machine by reporting a heartbeat at regular intervals. This service helps you identify running virtual machines that have stopped responding.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k ICService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Hyper-V PowerShell Direct Service

Name	vmicvmsession
Display Name	Hyper-V PowerShell Direct Service
Description	Provides a mechanism to manage virtual machine with PowerShell via VM session without a virtual network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies


Service Depends On	
--------------------	--

Log On


Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Hyper-V Time Synchronization Service


Name	vmictimesync
Display Name	Hyper-V Time Synchronization Service
Description	Synchronizes the system time of this virtual machine with the system time of the physical computer.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies

Service Depends On	VmGid
--------------------	-------

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Hyper-V Volume Shadow Copy Requestor

Name	vmicvss
Display Name	Hyper-V Volume Shadow Copy Requestor
Description	Coordinates the communications that are required to use Volume Shadow Copy Service to back up applications and data on this virtual machine from the operating system on the physical computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

IKE and AuthIP IPsec Keying Modules

Name	IKEEXT
Display Name	IKE and AuthIP IPsec Keying Modules
Description	The IKEEXT service hosts the Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are used for authentication and key exchange in Internet Protocol security (IPsec). Stopping or disabling the IKEEXT service will disable IKE and AuthIP key exchange with peer computers. IPsec is typically configured to use IKE or AuthIP; therefore, stopping or disabling the IKEEXT service might result in an IPsec failure and might compromise the security of the system. It is strongly recommended that you have the IKEEXT service running.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	BFE nsi
--------------------	------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Internet Connection Sharing (ICS)

Name	SharedAccess
Display Name	Internet Connection Sharing (ICS)
Description	Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	BFE
--------------------	-----

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

IP Helper

Name	iphlpvc
Display Name	IP Helper
Description	Provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Teredo), and IP-HTTPS. If this service is stopped, the computer will not have the enhanced connectivity benefits that these technologies offer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetSvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcSS tcpip nsi WinHttpAutoProxySvc
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

IPsec Policy Agent

Name	PolicyAgent
Display Name	IPsec Policy Agent
Description	Internet Protocol security (IPsec) supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. This service enforces IPsec policies created through the IP Security Policies snap-in or the command-line tool "netsh ipsec". If you stop this service, you may experience network connectivity issues if your policy requires that connections use IPsec. Also, remote management of Windows Defender Firewall is not available when this service is stopped.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	Tcpip bfe
--------------------	--------------

Log On

Account Name	NT Authority\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Services [J - R]

Displays the configuration of the Windows services on this machine

KDC Proxy Server service (KPS)

Name	KPSSVC
Display Name	KDC Proxy Server service (KPS)
Description	KDC Proxy Server service runs on edge servers to proxy Kerberos protocol messages to domain controllers on the corporate network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k KpsSvcGroup
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss http
--------------------	---------------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 KtmRm for Distributed Transaction Coordinator

Name	KtmRm
Display Name	KtmRm for Distributed Transaction Coordinator
Description	Coordinates transactions between the Distributed Transaction Coordinator (MSDTC) and the Kernel Transaction Manager (KTM). If it is not needed, it is recommended that this service remain stopped. If it is needed, both MSDTC and KTM will start this service automatically. If this service is disabled, any MSDTC transaction interacting with a Kernel Resource Manager will fail and any services that explicitly depend on it will fail to start.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetworkServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies

Service Depends On	RPCSS SamSS
--------------------	----------------

 Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	True

 Link-Layer Topology Discovery Mapper

Name	lltdsvc
Display Name	Link-Layer Topology Discovery Mapper
Description	Creates a Network Map, consisting of PC and device topology (connectivity) information, and metadata describing each PC and device. If this service is disabled, the Network Map will not function properly.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	rpcss lltdio
--------------------	-----------------

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Local Session Manager

Name	LSM
Display Name	Local Session Manager
Description	Core Windows Service that manages local user sessions. Stopping or disabling this service will result in system instability.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies


Service Depends On	RpcEptMapper DcomLaunch RpcSs
--------------------	-------------------------------------

Log On


Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 McpManagementService


Name	McpManagementService
Display Name	McpManagementService
Description	

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k McpManagementServiceGroup
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Enable Actions for Stops with Errors	False

Microsoft (R) Diagnostics Hub Standard Collector Service


Name	diagnosticshub.standardcollector.service
Display Name	Microsoft (R) Diagnostics Hub Standard Collector Service
Description	Diagnostics Hub Standard Collector Service. When running, this service collects real time ETW events and processes them.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Microsoft Account Sign-in Assistant

Name	wlidsvc
Display Name	Microsoft Account Sign-in Assistant
Description	Enables user sign-in through Microsoft account identity services. If this service is stopped, users will not be able to logon to the computer with their Microsoft account.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies


Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Microsoft App-V Client

Name	AppVClient
Display Name	Microsoft App-V Client
Description	Manages App-V users and virtual applications

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\AppVClient.exe
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	RpcSS netprofm AppVfs AppVStrm
--------------------	---

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Defender Antivirus Network Inspection Service

Name	WdNisSvc
Display Name	Microsoft Defender Antivirus Network Inspection Service
Description	Helps guard against intrusion attempts targeting known and newly discovered vulnerabilities in network protocols

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\NisSrv.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	WdNisDrv
--------------------	----------

Log On


Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 Microsoft Defender Antivirus Service


Name	WinDefend
Display Name	Microsoft Defender Antivirus Service
Description	Helps protect users from malware and other potentially unwanted software

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MsMpEng.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)


Name	MicrosoftEdgeElevationService
Display Name	Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)
Description	Keeps Microsoft Edge up to update. If this service is disabled, the application will not be kept up to date.

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Microsoft\Edge\Application\104.0.1293.70\elevation_service.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	RPCSS
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Edge Update Service (edgeupdate)

Name	edgeupdate
Display Name	Microsoft Edge Update Service (edgeupdate)
Description	Keeps your Microsoft software up to date. If this service is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Microsoft software using it.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Edge Update Service (edgeupdatem)

Name	edgeupdatem
Display Name	Microsoft Edge Update Service (edgeupdatem)
Description	Keeps your Microsoft software up to date. If this service is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Microsoft software using it.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /medsvc
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft iSCSI Initiator Service

Name	MSiSCSI
Display Name	Microsoft iSCSI Initiator Service
Description	Manages Internet SCSI (iSCSI) sessions from this computer to remote iSCSI target devices. If this service is stopped, this computer will not be able to login or access iSCSI targets. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	True

 Microsoft Passport

Name	NgcSvc
Display Name	Microsoft Passport
Description	Provides process isolation for cryptographic keys used to provide authentication to a user's associated identity providers. If this service is disabled, all uses and management of these keys will not be available, which includes machine log-on and single sign-on for apps and websites. This service starts and stops automatically. It is recommended that you do not reconfigure this service.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Microsoft Passport Container

Name	NgcCtrSvc
Display Name	Microsoft Passport Container
Description	Manages local user identity keys used to authenticate the user to identity providers, as well as TPM virtual smart cards. If this service is disabled, local user identity keys and TPM virtual smart cards will not be accessible. It is recommended that you do not reconfigure this service.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Microsoft Software Shadow Copy Provider

Name	swprv
Display Name	Microsoft Software Shadow Copy Provider
Description	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this service is stopped, software-based volume shadow copies cannot be managed. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k swprv
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Storage Spaces SMP

Name	smphost
Display Name	Microsoft Storage Spaces SMP
Description	Host service for the Microsoft Storage Spaces management provider. If this service is stopped or disabled, Storage Spaces cannot be managed.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k smphost
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Microsoft Store Install Service

Name	InstallService
Display Name	Microsoft Store Install Service
Description	Provides infrastructure support for the Microsoft Store. This service is started on demand, and if disabled then installations will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Net.Tcp Port Sharing Service

Name	NetTcpPortSharing
Display Name	Net.Tcp Port Sharing Service
Description	Provides ability to share TCP ports over the net.tcp protocol.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Netlogon


Name	Netlogon
Display Name	Netlogon
Description	Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\lsass.exe
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	LanmanWorkstation
--------------------	-------------------

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Network Connection Broker

Name	NcbService
Display Name	Network Connection Broker
Description	Brokers connections that allow Windows Store Apps to receive notifications from the internet.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

 Dependencies

Service Depends On	RpcSS tcpip BrokerInfrastructure
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Network Connections

Name	Netman
Display Name	Network Connections
Description	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	RpcSs nsi
--------------------	--------------

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Network Connectivity Assistant


Name	NcaSvc
Display Name	Network Connectivity Assistant
Description	Provides DirectAccess status notification for UI components

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetSvc -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies


Service Depends On	BFE dnscache NSI iphlpvc
--------------------	-----------------------------------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Network List Service

Name	netprofm
Display Name	Network List Service
Description	Identifies the networks the computer has connected to, collects and stores properties for these networks, and notifies applications when these properties change.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

 Dependencies


Service Depends On	RpcSs nlsvc
--------------------	----------------

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Network Location Awareness

Name	NlaSvc
Display Name	Network Location Awareness
Description	Collects and stores configuration information for the network and notifies programs when this information is modified. If this service is stopped, configuration information might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	NSI RpcSs TcpIp Dhcp Eventlog
--------------------	---

 Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Network Setup Service

Name	NetSetupSvc
Display Name	Network Setup Service
Description	The Network Setup Service manages the installation of network drivers and permits the configuration of low-level network settings. If this service is stopped, any driver installations that are in progress may be cancelled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Network Store Interface Service

Name	nsi
Display Name	Network Store Interface Service
Description	This service delivers network notifications (e.g. interface addition/deleting etc) to user mode clients. Stopping this service will cause loss of network connectivity. If this service is disabled, any other services that explicitly depend on this service will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss nsiproxy
--------------------	-------------------

Log On

Account Name	NT Authority\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Offline Files

Name	CscService
Display Name	Offline Files
Description	The Offline Files service performs maintenance activities on the Offline Files cache, responds to user logon and logoff events, implements the internals of the public API, and dispatches interesting events to those interested in Offline Files activities and changes in cache state.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 OpenSSH Authentication Agent


Name	ssh-agent
Display Name	OpenSSH Authentication Agent
Description	Agent to hold private keys used for public key authentication.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\OpenSSH\ssh-agent.exe
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies


Service Depends On	
--------------------	--

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Optimise drives

Name	defragsvc
Display Name	Optimise drives
Description	Helps the computer run more efficiently by optimising files on storage drives.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k defragsvc
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	RPCSS
--------------------	-------

 Log On


Account Name	localSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Payments and NFC/SE Manager

Name	SEMgrSvc
Display Name	Payments and NFC/SE Manager
Description	Manages payments and Near Field Communication (NFC) based secure elements.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Performance Counter DLL Host

Name	PerfHost
Display Name	Performance Counter DLL Host
Description	Enables remote users and 64-bit processes to query performance counters provided by 32-bit DLLs. If this service is stopped, only local users and 32-bit processes will be able to query performance counters provided by 32-bit DLLs.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\SysWow64\perfhost.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

☰ Performance Logs & Alerts

Name	pla
Display Name	Performance Logs & Alerts
Description	Performance Logs and Alerts Collects performance data from local or remote computers based on preconfigured schedule parameters, then writes the data to a log or triggers an alert. If this service is stopped, performance information will not be collected. If this service is disabled, any services that explicitly depend on it will fail to start.

🔧 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

🔗 Dependencies

Service Depends On	RPCSS
--------------------	-------

👤 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

🔄 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 PimIndexMaintenanceSvc_526cb


Name	PimIndexMaintenanceSvc_526cb
Display Name	PimIndexMaintenanceSvc_526cb
Description	Indexes contact data for fast contact searching. If you stop or disable this service, contacts might be missing from your search results.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	
--------------------	--

 Log On

Account Name	
--------------	--

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Plug and Play


Name	PlugPlay
Display Name	Plug and Play
Description	Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Portable Device Enumerator Service

Name	WPDBusEnum
Display Name	Portable Device Enumerator Service
Description	Enforces group policy for removable mass-storage devices. Enables applications such as Windows Media Player and Image Import Wizard to transfer and synchronize content using removable mass-storage devices.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On


Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Power


Name	Power
Display Name	Power
Description	Manages power policy and power policy notification delivery.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies


Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Computer
Second Failure Action	Restart the Computer
Subsequent Failure Action	Restart the Computer
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	1 minutes

 Print Spooler


Name	Spooler
Display Name	Print Spooler
Description	This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't be able to print or see your printers.

 Advanced

Allow Interaction With Desktop	True
Path Name	C:\Windows\System32\spoolsv.exe
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	RPCSS http
--------------------	---------------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Printer Extensions and Notifications

Name	PrintNotify
Display Name	Printer Extensions and Notifications
Description	This service opens custom printer dialogue boxes and handles notifications from a remote print server or a printer. If you turn this service off, you won't be able to see printer extensions or notifications.

 Advanced

Allow Interaction With Desktop	True
Path Name	C:\Windows\system32\svchost.exe -k print
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

PrintWorkflowUserSvc_526cb

Name	PrintWorkflowUserSvc_526cb
Display Name	PrintWorkflowUserSvc_526cb
Description	Provides support for Print Workflow applications. If you turn off this service, you may not be able to print successfully.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k PrintWorkflow
Service Execution Type	Unknown
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies


Service Depends On	
--------------------	--

 Log On

Account Name	
--------------	--

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Problem Reports Control Panel Support


Name	wercplsupport
Display Name	Problem Reports Control Panel Support
Description	This service provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports control panel.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	localSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Program Compatibility Assistant Service

Name	PcaSvc
Display Name	Program Compatibility Assistant Service
Description	This service provides support for the Program Compatibility Assistant (PCA). PCA monitors programs installed and run by the user and detects known compatibility problems. If this service is stopped, PCA will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 Quality Windows Audio Video Experience

Name	QWAVE
Display Name	Quality Windows Audio Video Experience
Description	Quality Windows Audio Video Experience (qWave) is a networking platform for Audio Video (AV) streaming applications on IP home networks. qWave enhances AV streaming performance and reliability by ensuring network quality-of-service (QoS) for AV applications. It provides mechanisms for admission control, run time monitoring and enforcement, application feedback, and traffic prioritization.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	rpcss psched QWAVEdrv LLTDIO
--------------------	---------------------------------------

 Log On


Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Radio Management Service


Name	RmSvc
Display Name	Radio Management Service
Description	Radio Management and Airplane Mode Service

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Remote Access Auto Connection Manager


Name	RasAuto
Display Name	Remote Access Auto Connection Manager
Description	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	RasAcd
--------------------	--------

 Log On

Account Name	localSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Remote Access Connection Manager

Name	RasMan
Display Name	Remote Access Connection Manager
Description	Manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	SstpSvc DnsCache
--------------------	---------------------

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Remote Desktop Configuration

Name	SessionEnv
Display Name	Remote Desktop Configuration
Description	Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop Services and Remote Desktop related configuration and session maintenance activities that require SYSTEM context. These include per-session temporary folders, RD themes, and RD certificates.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS LanmanWorkstation
--------------------	----------------------------

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Remote Desktop Services

Name	TermService
Display Name	Remote Desktop Services
Description	Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the checkboxes on the Remote tab of the System properties control panel item.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k termsvcs
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies


Service Depends On	RPCSS
--------------------	-------

Log On


Account Name	NT Authority\NetworkService
--------------	-----------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 Remote Desktop Services UserMode Port Redirector


Name	UmRdpService
Display Name	Remote Desktop Services UserMode Port Redirector
Description	Allows the redirection of Printers/Drives/Ports for RDP connections

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	TermService RDPDR
--------------------	----------------------

 Log On

Account Name	localSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Remote Procedure Call (RPC)

Name	RpcSs
Display Name	Remote Procedure Call (RPC)
Description	The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activations requests, object exporter resolutions and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k rpcss -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RpcEptMapper DcomLaunch
--------------------	----------------------------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	1 minutes

Remote Procedure Call (RPC) Locator

Name	RpcLocator
Display Name	Remote Procedure Call (RPC) Locator
Description	In Windows 2003 and earlier versions of Windows, the Remote Procedure Call (RPC) Locator service manages the RPC name service database. In Windows Vista and later versions of Windows, this service does not provide any functionality and is present for application compatibility.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\locator.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Remote Registry

Name	RemoteRegistry
Display Name	Remote Registry
Description	Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k localService -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Stopped

Dependencies


Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 Resultant Set of Policy Provider


Name	RSoPProv
Display Name	Resultant Set of Policy Provider
Description	Provides a network service that processes requests to simulate application of Group Policy settings for a target user or computer in various situations and computes the Resultant Set of Policy settings.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\RSoPProv.exe
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	RPCSS
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Routing and Remote Access

Name	RemoteAccess
Display Name	Routing and Remote Access
Description	Offers routing services to businesses in local area and wide area network environments.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	RpcSS Bfe RasMan Http
--------------------	--------------------------------

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

RPC Endpoint Mapper

Name	RpcEptMapper
Display Name	RPC Endpoint Mapper
Description	Resolves RPC interfaces identifiers to transport endpoints. If this service is stopped or disabled, programs using Remote Procedure Call (RPC) services will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k RPCSS -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Services [S - Z]

Displays the configuration of the Windows services on this machine

Secondary Log-on

Name	seclogon
Display Name	Secondary Log-on
Description	Enables starting processes under alternate credentials. If this service is stopped, this type of log-on access will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Secure Socket Tunneling Protocol Service

Name	SstpSvc
Display Name	Secure Socket Tunneling Protocol Service
Description	Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT Authority\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Security Accounts Manager

Name	SamSs
Display Name	Security Accounts Manager
Description	The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\lsass.exe
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On


Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Sensor Data Service

Name	SensorDataService
Display Name	Sensor Data Service
Description	Delivers data from a variety of sensors

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\SensorDataService.exe
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

☰ Sensor Monitoring Service

Name	SensrSvc
Display Name	Sensor Monitoring Service
Description	Monitors various sensors in order to expose data and adapt to system and user state. If this service is stopped or disabled, the display brightness will not adapt to lighting conditions. Stopping this service may affect other system functionality and features as well.

🔑 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

🔗 Dependencies

Service Depends On	
--------------------	--

👤 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

🔄 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

☰ Sensor Service

Name	SensorService
Display Name	Sensor Service
Description	A service for sensors that manages different sensors' functionality. Manages Simple Device Orientation (SDO) and History for sensors. Loads the SDO sensor that reports device orientation changes. If this service is stopped or disabled, the SDO sensor will not be loaded and so auto-rotation will not occur. History collection from Sensors will also be stopped.

🔧 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

🔗 Dependencies

Service Depends On	
--------------------	--

👤 Log On

Account Name	LocalSystem
--------------	-------------

🔄 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Server

Name	LanmanServer
Display Name	Server
Description	Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k smbsvcs
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	SamSS Srv2
--------------------	---------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

 Shared PC Account Manager


Name	shpamsvc
Display Name	Shared PC Account Manager
Description	Manages profiles and accounts on a SharedPC configured device

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

 Dependencies


Service Depends On	RpcSs ProfSvc
--------------------	------------------

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Shell Hardware Detection

Name	ShellHWDetection
Display Name	Shell Hardware Detection
Description	Provides notifications for AutoPlay hardware events.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Smart Card

Name	SCardSvr
Display Name	Smart Card
Description	Manages access to smart cards read by this computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Smart Card Device Enumeration Service

Name	ScDeviceEnum
Display Name	Smart Card Device Enumeration Service
Description	Creates software device nodes for all smart card readers accessible to a given session. If this service is disabled, WinRT APIs will not be able to enumerate smart card readers.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies


Service Depends On	
--------------------	--

Log On


Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Smart Card Removal Policy

Name	SCPolicySvc
Display Name	Smart Card Removal Policy
Description	Allows the system to be configured to lock the user desktop upon smart card removal.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

☰ SNMP Trap

Name	SNMPTRAP
Display Name	SNMP Trap
Description	Receives trap messages generated by local or remote Simple Network Management Protocol (SNMP) agents and forwards the messages to SNMP management programs running on this computer. If this service is stopped, SNMP-based programs on this computer will not receive SNMP trap messages. If this service is disabled, any services that explicitly depend on it will fail to start.

🔧 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\snmptrap.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

🔗 Dependencies

Service Depends On	
--------------------	--

👤 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

🔄 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Software Protection

Name	sppsvc
Display Name	Software Protection
Description	Enables the download, installation and enforcement of digital licenses for Windows and Windows applications. If the service is disabled, the operating system and licensed applications may run in a notification mode. It is strongly recommended that you not disable the Software Protection service.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\sppsvc.exe
Service Execution Type	Own Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Special Administration Console Helper

Name	sacsvr
Display Name	Special Administration Console Helper
Description	Allows administrators to remotely access a command prompt using Emergency Management Services.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies


Service Depends On	
--------------------	--

Log On


Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

 Spot Verifier


Name	svsvc
Display Name	Spot Verifier
Description	Verifies potential file system corruptions.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

SQL Server (SQLEXPRESS)

Name	MSSQL\$SQLEXPRESS
Display Name	SQL Server (SQLEXPRESS)
Description	Provides storage, processing and controlled access of data, and rapid transaction processing.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\Binn\sqlservr.exe" -sSQLEXPRESS
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	KEYISO
--------------------	--------

Log On


Account Name	NT Service\MSSQL\$SQLEXPRESS
--------------	------------------------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 SQL Server Agent (SQLEXPRESS)


Name	SQLAgent\$SQLEXPRESS
Display Name	SQL Server Agent (SQLEXPRESS)
Description	Executes jobs, monitors SQL Server, fires alerts, and allows automation of some administrative tasks.

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\Binn\SQLAGENT.EXE" -i SQLEXPRESS
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	MSSQL\$SQLEXPRESS
--------------------	-------------------

 Log On

Account Name	NT AUTHORITY\NETWORKSERVICE
--------------	-----------------------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 SQL Server Browser

Name	SQLBrowser
Display Name	SQL Server Browser
Description	Provides SQL Server connection information to client computers.

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe"
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	NT AUTHORITY\LOCALSERVICE
--------------	---------------------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

SQL Server CEIP service (SQLEXPRESS)

Name	SQLTELEMETRY\$SQLEXPRESS
Display Name	SQL Server CEIP service (SQLEXPRESS)
Description	CEIP service for Sql server

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\Binn\sqlceip.exe" -Service SQLEXPRESS
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT Service\SQLTELEMETRY\$SQLEXPRESS
--------------	-------------------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

SQL Server VSS Writer

Name	SQLWriter
Display Name	SQL Server VSS Writer
Description	Provides the interface to backup/restore Microsoft SQL server through the Windows VSS infrastructure.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

SSDP Discovery

Name	SSDPSRV
Display Name	SSDP Discovery
Description	Discovers networked devices and services that use the SSDP discovery protocol, such as UPnP devices. Also announces SSDP devices and services running on the local computer. If this service is stopped, SSDP-based devices will not be discovered. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies


Service Depends On	HTTP NSI
--------------------	-------------

Log On


Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 State Repository Service


Name	StateRepository
Display Name	State Repository Service
Description	Provides required infrastructure support for the application model.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k appmodel -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies


Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Still Image Acquisition Events

Name	WiaRpc
Display Name	Still Image Acquisition Events
Description	Launches applications associated with still image acquisition events.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	RpcSs
--------------------	-------

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Storage Service


Name	StorSvc
Display Name	Storage Service
Description	Provides enabling services for storage settings and external storage expansion

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start, Trigger Start)
Service State	Running

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Storage Tiers Management

Name	TieringEngineService
Display Name	Storage Tiers Management
Description	Optimizes the placement of data in storage tiers on all tiered storage spaces in the system.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\TieringEngineService.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	
--------------------	--

 Log On

Account Name	localSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 SysMain


Name	SysMain
Display Name	SysMain
Description	Maintains and improves system performance over time.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies


Service Depends On	rpcss
--------------------	-------

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 System Event Notification Service

Name	SENS
Display Name	System Event Notification Service
Description	Monitors system events and notifies subscribers to COM+ Event System of these events.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	EventSystem
--------------------	-------------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

System Events Broker

Name	SystemEventsBroker
Display Name	System Events Broker
Description	Coordinates execution of background work for WinRT application. If this service is stopped or disabled, then background work might not be triggered.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcEptMapper RpcSs
--------------------	-----------------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Computer
Second Failure Action	Restart the Computer
Subsequent Failure Action	Restart the Computer
Reset Failure Count	1 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	2 minutes

 System Guard Runtime Monitor Broker

Name	SgrmBroker
Display Name	System Guard Runtime Monitor Broker
Description	Monitors and attests to the integrity of the Windows platform.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\SgrmBroker.exe
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Task Scheduler

Name	Schedule
Display Name	Task Scheduler
Description	Enables a user to configure and schedule automated tasks on this computer. The service also hosts multiple Windows system-critical tasks. If this service is stopped or disabled, these tasks will not be run at their scheduled times. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RPCSS SystemEventsBroker
--------------------	-----------------------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Unknown
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

☰ TCP/IP NetBIOS Helper

Name	lmhosts
Display Name	TCP/IP NetBIOS Helper
Description	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on the network, therefore enabling users to share files, print, and log on to the network. If this service is stopped, these functions might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

🔧 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

🔗 Dependencies

Service Depends On	Afd
--------------------	-----

👤 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

🔄 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Telephony

Name	tapisrv
Display Name	Telephony
Description	Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also running the service.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On


Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Themes

Name	Themes
Display Name	Themes
Description	Provides user experience theme management.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies


Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 Time Broker


Name	TimeBrokerSvc
Display Name	Time Broker
Description	Coordinates execution of background work for WinRT application. If this service is stopped or disabled, then background work might not be triggered.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

 Dependencies


Service Depends On	
--------------------	--

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Touch Keyboard and Handwriting Panel Service


Name	TabletInputService
Display Name	Touch Keyboard and Handwriting Panel Service
Description	Enables Touch Keyboard and Handwriting Panel pen and ink functionality

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

UdkUserSvc_526cb

Name	UdkUserSvc_526cb
Display Name	UdkUserSvc_526cb
Description	Shell components service

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k UdkSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	
--------------	--

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

☰ UnistoreSvc_526cb

Name	UnistoreSvc_526cb
Display Name	UnistoreSvc_526cb
Description	Handles storage of structured user data, including contact info, calendars, messages and other content. If you stop or disable this service, apps that use this data might not work correctly.

🔧 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

🔗 Dependencies

Service Depends On	
--------------------	--

👤 Log On

Account Name	
--------------	--

🔄 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Update Orchestrator Service


Name	UsoSvc
Display Name	Update Orchestrator Service
Description	Manages Windows Updates. If stopped, your devices will not be able to download and install the latest updates.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

UPnP Device Host

Name	upnphost
Display Name	UPnP Device Host
Description	Allows UPnP devices to be hosted on this computer. If this service is stopped, any hosted UPnP devices will stop functioning and no additional hosted devices can be added. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	SSDPSRV HTTP
--------------------	-----------------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

User Access Logging Service

Name	UALSVC
Display Name	User Access Logging Service
Description	This service logs unique client access requests, in the form of IP addresses and user names, of installed products and roles on the local server. This information can be queried, via Powershell, by administrators needing to quantify client demand of server software for offline Client Access License (CAL) management. If the service is disabled, client requests will not be logged and will not be retrievable via Powershell queries. Stopping the service will not affect query of historical data (see supporting documentation for steps to delete historical data). The local system administrator must consult his, or her, Windows Server license terms to determine the number of CALs that are required for the server software to be appropriately licensed; use of the UAL service and data does not alter this obligation.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic (Delayed Start)
Service State	Running

Dependencies


Service Depends On	WinMgmt
--------------------	---------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 User Experience Virtualization Service

Name	UevAgentService
Display Name	User Experience Virtualization Service
Description	Provides support for application and OS settings roaming

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\AgentService.exe
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

User Manager

Name	UserManager
Display Name	User Manager
Description	User Manager provides the runtime components required for multi-user interaction. If this service is stopped, some applications may not operate correctly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs ProfSvc
--------------------	------------------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

☰ User Profile Service

Name	ProfSvc
Display Name	User Profile Service
Description	This service is responsible for loading and unloading user profiles. If this service is stopped or disabled, users will no longer be able to successfully sign in or sign out, apps might have problems getting to users' data, and components registered to receive profile event notifications won't receive them.

🔑 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

🔗 Dependencies

Service Depends On	RpcSs
--------------------	-------

👤 Log On

Account Name	LocalSystem
--------------	-------------

🔄 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

☰ UserDataSvc_526cb

Name	UserDataSvc_526cb
Display Name	UserDataSvc_526cb
Description	Provides apps with access to structured user data, including contact info, calendars, messages and other content. If you stop or disable this service, apps that use this data might not work correctly.

🔧 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Manual
Service State	Stopped

🔗 Dependencies


Service Depends On	
--------------------	--

👤 Log On


Account Name	
--------------	--

🔄 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Virtual Disk


Name	vds
Display Name	Virtual Disk
Description	Provides management services for disks, volumes, file systems, and storage arrays.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\vds.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	RpcSs
--------------------	-------

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

 VMware Alias Manager and Ticket Service


Name	VGAuthService
Display Name	VMware Alias Manager and Ticket Service
Description	Alias Manager and Ticket Service

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	
--------------------	--

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 VMware Snapshot Provider

Name	vmvss
Display Name	VMware Snapshot Provider
Description	VMware Snapshot Provider

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\dlhhost.exe /Processid:{512485CC-E5DB-4112-AB76-DBE47ABE6CBB}
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 VMware SVGA Helper Service

Name	vm3dservice
Display Name	VMware SVGA Helper Service
Description	Helps VMware SVGA driver by collecting and conveying user mode information

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\vm3dservice.exe
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

 Dependencies


Service Depends On	
--------------------	--

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 VMware Tools

Name	VMTools
Display Name	VMware Tools
Description	Provides support for synchronizing objects between the host and guest operating systems.

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Volume Shadow Copy

Name	VSS
Display Name	Volume Shadow Copy
Description	Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\vssvc.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

W3C Logging Service

Name	w3logsvc
Display Name	W3C Logging Service
Description	Provides W3C logging for Internet Information Services (IIS). If this service is stopped, W3C logging configured by IIS will not work.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k apphost
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies


Service Depends On	HTTP
--------------------	------

Log On


Account Name	localSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 WalletService


Name	WalletService
Display Name	WalletService
Description	Hosts objects used by clients of the wallet

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k appmodel -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Warp JIT Service

Name	WarpJITSvc
Display Name	Warp JIT Service
Description	Enables JIT compilation support in d3d10warp.dll for processes in which code generation is disabled.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies


Service Depends On	
--------------------	--

Log On


Account Name	NT Authority\LocalService
--------------	---------------------------

Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Web Account Manager


Name	TokenBroker
Display Name	Web Account Manager
Description	This service is used by Web Account Manager to provide single-sign-on to apps and services.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

 Dependencies

Service Depends On	UserManager BrokerInfrastructure
--------------------	-------------------------------------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Web Management Service

Name	WMSVC
Display Name	Web Management Service
Description	The Web Management Service enables remote and delegated management capabilities for administrators to manage for the Web server, sites and applications present on this machine.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\inetsrv\wmsvc.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies


Service Depends On	HTTP
--------------------	------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 Windows Audio

Name	Audiosrv
Display Name	Windows Audio
Description	Manages audio for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	AudioEndpointBuilder RpcSs
--------------------	-------------------------------

 Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	3 minutes
Enable Actions for Stops with Errors	False

Windows Audio Endpoint Builder

Name	AudioEndpointBuilder
Display Name	Windows Audio Endpoint Builder
Description	Manages audio devices for the Windows Audio service. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Windows Biometric Service

Name	WbioSvc
Display Name	Windows Biometric Service
Description	The Windows biometric service gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k WbioSvcGroup
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

Dependencies

Service Depends On	RpcSs
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Camera Frame Server

Name	FrameServer
Display Name	Windows Camera Frame Server
Description	Enables multiple clients to access video frames from camera devices.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k Camera
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Camera Frame Server Monitor

Name	FrameServerMonitor
Display Name	Windows Camera Frame Server Monitor
Description	Monitors the health and state for the Windows Camera Frame Server service.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k CameraMonitor
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	3 minutes
Enable Actions for Stops with Errors	False

 Windows Connection Manager

Name	Wcmsvc
Display Name	Windows Connection Manager
Description	Makes automatic connect/disconnect decisions based on the network connectivity options currently available to the PC and enables management of network connectivity based on Group Policy settings.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Own Process
Start Mode	Automatic (Trigger Start)
Service State	Running

 Dependencies

Service Depends On	RpcSs NSI
--------------------	--------------

 Log On

Account Name	NT Authority\LocalService
--------------	---------------------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Defender Advanced Threat Protection Service

Name	Sense
Display Name	Windows Defender Advanced Threat Protection Service
Description	Windows Defender Advanced Threat Protection service helps protect against advanced threats by monitoring and reporting security events that happen on the computer.

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Defender Firewall

Name	mpssvc
Display Name	Windows Defender Firewall
Description	Windows Defender Firewall helps to protect your computer by preventing unauthorised users from gaining access to your computer through the Internet or a network.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	mpsdrv bfe nsi
--------------------	----------------------

Log On

Account Name	NT Authority\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Computer
Second Failure Action	Restart the Computer
Subsequent Failure Action	Restart the Computer
Reset Failure Count	1 days
Enable Actions for Stops with Errors	False
Computer Restart Delay	1 minutes

Windows Encryption Provider Host Service

Name	WEPHOSTSVC
Display Name	Windows Encryption Provider Host Service
Description	Windows Encryption Provider Host Service brokers encryption related functionalities from 3rd Party Encryption Providers to processes that need to evaluate and apply EAS policies. Stopping this will compromise EAS compliancy checks that have been established by the connected Mail Accounts

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k WepHostSvcGroup
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Error Reporting Service

Name	WerSvc
Display Name	Windows Error Reporting Service
Description	Allows errors to be reported when programs stop working or responding and allows existing solutions to be delivered. Also allows logs to be generated for diagnostic and repair services. If this service is stopped, error reporting might not work correctly and results of diagnostic services and repairs might not be displayed.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k WerSvcGroup
Service Execution Type	Own Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Event Collector

Name	Wecsvc
Display Name	Windows Event Collector
Description	This service manages persistent subscriptions to events from remote sources that support WS-Management protocol. This includes Windows Vista event logs, hardware and IPMI-enabled event sources. The service stores forwarded events in a local Event Log. If this service is stopped or disabled event subscriptions cannot be created and forwarded events cannot be accepted.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	HTTP Eventlog
--------------------	------------------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Event Log

Name	EventLog
Display Name	Windows Event Log
Description	This service manages events and event logs. It supports logging events, querying events, subscribing to events, archiving event logs, and managing event metadata. It can display events in both XML and plain text format. Stopping this service may compromise security and reliability of the system.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	True

Windows Font Cache Service

Name	FontCache
Display Name	Windows Font Cache Service
Description	Optimizes performance of applications by caching commonly used font data. Applications will start this service if it is not already running. It can be disabled, though doing so will degrade application performance.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies


Service Depends On	
--------------------	--

Log On


Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

 Windows Image Acquisition (WIA)

Name	StiSvc
Display Name	Windows Image Acquisition (WIA)
Description	Provides image acquisition services for scanners and cameras

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k imgsvc
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	NT Authority\LocalService
--------------	---------------------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Windows Insider Service


Name	wisvc
Display Name	Windows Insider Service
Description	Provides infrastructure support for the Windows Insider Programme. This service must remain enabled for the Windows Insider Programme to work.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

 Dependencies


Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 Windows Installer

Name	msiserver
Display Name	Windows Installer
Description	Adds, modifies and removes applications provided as a Windows Installer or APPX package (*.msi, *.msp, *.appx). If this service is disabled, any services that explicitly depend on it will fail to start.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\msiexec.exe /V
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

 Dependencies


Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Windows License Manager Service


Name	LicenseManager
Display Name	Windows License Manager Service
Description	Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled then content acquired through the Microsoft Store will not function properly.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k LocalService -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Running

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	NT Authority\LocalService
--------------	---------------------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows Management Instrumentation

Name	Winmgmt
Display Name	Windows Management Instrumentation
Description	Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	RPCSS
--------------------	-------

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows Media Player Network Sharing Service

Name	WMPNetworkSvc
Display Name	Windows Media Player Network Sharing Service
Description	Shares Windows Media Player libraries with other networked players and media devices using Universal Plug and Play

Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\Windows Media Player\wmpnetwk.exe"
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	http WSearch
--------------------	-----------------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Windows Modules Installer

Name	TrustedInstaller
Display Name	Windows Modules Installer
Description	Enables installation, modification, and removal of Windows updates and optional components. If this service is disabled, install or uninstall of Windows updates might fail for this computer.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\servicing\TrustedInstaller.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies


Service Depends On	
--------------------	--

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Windows Process Activation Service


Name	WAS
Display Name	Windows Process Activation Service
Description	The Windows Process Activation Service (WAS) provides process activation, resource management and health management services for message-activated applications.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k iissvcs
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

 Dependencies

Service Depends On	RPCSS
--------------------	-------

 Log On

Account Name	localSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Windows Push Notifications System Service

Name	WpnService
Display Name	Windows Push Notifications System Service
Description	This service runs in session 0 and hosts the notification platform and connection provider which handles the connection between the device and WNS server.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Windows PushToInstall Service

Name	PushToInstall
Display Name	Windows PushToInstall Service
Description	Provides infrastructure support for the Microsoft Store. This service is started automatically and if disabled then remote installations will not function properly.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Disabled
Service State	Stopped

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Windows Remote Management (WS-Management)

Name	WinRM
Display Name	Windows Remote Management (WS-Management)
Description	Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The WinRM Service needs to be configured with a listener using winrm.cmd command line tool or through Group Policy in order for it to listen over the network. The WinRM service provides access to WMI data and enables event collection. Event collection and subscription to events require that the service is running. WinRM messages use HTTP and HTTPS as transports. The WinRM service does not depend on IIS but is preconfigured to share a port with IIS on the same machine. The WinRM service reserves the /wsman URL prefix. To prevent conflicts with IIS, administrators should ensure that any websites hosted on IIS do not use the /wsman URL prefix.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies


Service Depends On	RPCSS HTTP
--------------------	---------------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

 Windows Search

Name	WSearch
Display Name	Windows Search
Description	Provides content indexing, property caching, and search results for files, e-mail, and other content.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\SearchIndexer.exe /Embedding
Service Execution Type	Own Process
Start Mode	Disabled
Service State	Stopped

 Dependencies

Service Depends On	RPCSS BrokerInfrastructure
--------------------	-------------------------------

 Log On


Account Name	LocalSystem
--------------	-------------

 Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	True

 Windows Security Service

Name	SecurityHealthService
Display Name	Windows Security Service
Description	Windows Security Service handles unified device protection and health information

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\SecurityHealthService.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Running

 Dependencies

Service Depends On	RpcSs
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

Windows Time

Name	W32Time
Display Name	Windows Time
Description	Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalService
Service Execution Type	Share Process
Start Mode	Automatic (Trigger Start)
Service State	Running

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

Windows Update

Name	wuauerv
Display Name	Windows Update
Description	Enables the detection, download and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k netsvcs -p
Service Execution Type	Share Process
Start Mode	Manual (Trigger Start)
Service State	Stopped

Dependencies

Service Depends On	rpcss
--------------------	-------

Log On

Account Name	LocalSystem
--------------	-------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	1 minutes
Enable Actions for Stops with Errors	False

 Windows Update Medic Service


Name	WaaSMedicSvc
Display Name	Windows Update Medic Service
Description	Enables remediation and protection of Windows Update components.

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k wusvcs -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

 Dependencies

Service Depends On	rpcss
--------------------	-------

 Log On

Account Name	LocalSystem
--------------	-------------

 Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

WinHTTP Web Proxy Auto-Discovery Service

Name	WinHttpAutoProxySvc
Display Name	WinHTTP Web Proxy Auto-Discovery Service
Description	WinHTTP implements the client HTTP stack and provides developers with a Win32 API and COM Automation component for sending HTTP requests and receiving responses. In addition, WinHTTP provides support for auto-discovering a proxy configuration via its implementation of the Web Proxy Auto-Discovery (WPAD) protocol.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Running

Dependencies

Service Depends On	Dhcp
--------------------	------

Log On

Account Name	NT AUTHORITY\LocalService
--------------	---------------------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	1000 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

Wired AutoConfig

Name	dot3svc
Display Name	Wired AutoConfig
Description	The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Service Execution Type	Share Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	RpcSs Ndisuio Eaphost
--------------------	-----------------------------

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

WMI Performance Adapter

Name	wmiApSrv
Display Name	WMI Performance Adapter
Description	Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\wbem\WmiApSrv.exe
Service Execution Type	Own Process
Start Mode	Manual
Service State	Stopped

Dependencies

Service Depends On	
--------------------	--

Log On

Account Name	localSystem
--------------	-------------

Recovery

First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Service Restart Delay	5 minutes
Enable Actions for Stops with Errors	False

Workstation

Name	LanmanWorkstation
Display Name	Workstation
Description	Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\System32\svchost.exe -k NetworkService -p
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

Dependencies

Service Depends On	Browser MRxSmb20 NSI
--------------------	----------------------------

Log On

Account Name	NT AUTHORITY\NetworkService
--------------	-----------------------------

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Take No action
Reset Failure Count	1 days
Service Restart Delay	2 minutes
Enable Actions for Stops with Errors	False

 World Wide Web Publishing Service


Name	W3SVC
Display Name	World Wide Web Publishing Service
Description	Provides Web connectivity and administration through the Internet Information Services Manager

 Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k iissvcs
Service Execution Type	Share Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	WAS HTTP
--------------------	-------------

 Log On

Account Name	localSystem
--------------	-------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

WpnUserService_526cb

Name	WpnUserService_526cb
Display Name	WpnUserService_526cb
Description	This service hosts the Windows notification platform which provides support for local and push notifications. Supported notifications are tile, toast and raw.

Advanced

Allow Interaction With Desktop	False
Path Name	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Service Execution Type	Unknown
Start Mode	Automatic
Service State	Running

Dependencies


Service Depends On	
--------------------	--

Log On

Account Name	
--------------	--

Recovery


First Failure Action	Restart the Service
Second Failure Action	Restart the Service
Subsequent Failure Action	Restart the Service
Reset Failure Count	1 days
Service Restart Delay	0 minutes
Enable Actions for Stops with Errors	False

 XIA Configuration Scheduler


Name	XCSSchedulerService
Display Name	XIA Configuration Scheduler
Description	Schedules actions on the XIA Configuration Server.

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Scheduler\CENTREL.XIA.Configuration.Server.Scheduler.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

 Dependencies


Service Depends On	W3SVC
--------------------	-------

 Log On


Account Name	NT AUTHORITY\NETWORK SERVICE
--------------	------------------------------

 Recovery


First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

 XIA Configuration Service


Name	XIAConfigurationSvc
Display Name	XIA Configuration Service
Description	Accesses and documents network devices for the CENTREL Solutions - XIA Configuration Server

 Advanced

Allow Interaction With Desktop	False
Path Name	"C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe"
Service Execution Type	Own Process
Start Mode	Automatic
Service State	Running

 Dependencies

Service Depends On	
--------------------	--

 Log On

Account Name	TEST2022\sysadmin
--------------	-------------------

 Recovery

First Failure Action	Take No action
Second Failure Action	Take No action
Subsequent Failure Action	Take No action
Reset Failure Count	0 days
Enable Actions for Stops with Errors	False

Windows 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	